(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 May 2001 (03.05.2001)

PCT

(10) International Publication Number
WO 01/31849 A1

(51) International Patent Classification[7]: H04L 12/24

(21) International Application Number: PCT/US00/29689

(22) International Filing Date: 26 October 2000 (26.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/429,504 27 October 1999 (27.10.1999) US

(71) Applicant: **MICRO WEB SERVERS** [US/US]; 2800 Industrial Terrace, Austin, TX 78758 (US).

(72) Inventors: **FOWLER, John, J.**; 4805 Avenue G, Apartment A, Austin, TX 78751 (US). **CULLEN, Gerard, L.**; 1707 Spy Glass Drive, #52, Austin, TX 78758 (US).

(74) Agent: **PASTRANA, Armando**; Gray Cary Ware & Freidenrich LLP, Suite 1440, 100 Congress Avenue, Austin, TX 78701 (US).

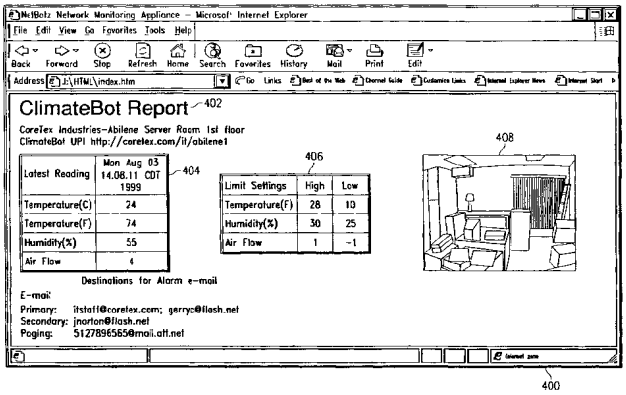
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR MONITORING COMPUTER NETWORKS AND EQUIPMENT



(57) Abstract: A system and method are disclosed for monitoring a space and its contents over a network. The system can include an embedded Java microprocessor to provide processing and network connectivity capability, and sensors to detect physical parameters associated with the space. The sensors can generate one or more sensor signals representative of the detected physical parameters. An analog-to-digital converter can convert the sensor signals to a digital format and can provide corresponding digital signals to the microprocessor. The system further includes instructions for processing the sensor signals and corresponding digital signals. An alarm signal can be generated when any of the physical parameters exceeds a corresponding threshold value. The system of the present invention can have at least one input/output port for communicating with the network and one or more memory modules for storing system data. The system of this invention can have a network-based interface for providing programming instructions to the microprocessor and for receiving monitoring status and alarm information from the system. The interface can be an HTML interface. A power source provides power to the system.

WO 01/31849 A1

DESCRIPTION

METHOD AND SYSTEM FOR MONITORING COMPUTER NETWORKS AND EQUIPMENT

TECHNICAL FIELD OF THE INVENTION

The present invention relates generally to computer network and equipment monitoring systems and methods and, more particularly, to computer network monitoring systems that can be accessed locally or remotely. Even more particularly, the present invention relates to a computer network and equipment monitoring system that can provide real-time status of environmental conditions, alarm functions, and real-time video imaging of a space or equipment being monitored over a global network, such as the internet.

BACKGROUND OF THE INVENTION

Data traffic on networks, particularly on the internet, has increased dramatically over the past several years, and this trend will continue with the rapid growth of e-commerce and other services on the internet requiring greater bandwidth. With this increase in data traffic on networks, there has been a corresponding increase in the number of computer equipment rooms, known as "server rooms," used to house the equipment necessary to support data traffic routing. Furthermore, the increasing dependency of companies on their internet presence has created an urgency to keep the server rooms up and running at all times. Industry estimates show that there are over 400,000 such rooms currently in existence in the United States.

The growth in internet traffic has prompted many businesses to construct a server room to allow their employees to access internet information or enable e-commerce and store data. Once viewed as a goal, continuous server up time has become a necessity. Keeping track of numerous computers, along with associated bridges, routers, backup power supplies, etc., can be a formidable task. A large company with server rooms in more than one city might well be faced with spending thousands of dollars on software packages to keep their equipment running. Prices of $1,000 per computer are common. Dedicated technicians are also needed to monitor network equipment and issue work orders to repair failed units.

While reliable, modern computer systems cannot tolerate excess heat, dust or humidity. Heat can rapidly cause equipment deterioration. Failure of CPU cooling fans can reduce equipment lifetime to days or hours. A single high-speed LAN (local area network) failure can cause slow system response. These and other such failures within the equipment in a server room occur routinely and can cause great disruption to a business.

Solutions do currently exist for monitoring computer networks and equipment to prevent such failures. However, these solutions are primarily targeted at high-end, very large systems such as those used by large corporations or institutions that have large budgets to support equipment monitoring. For example, Hewlett-Packard provides a high-end monitoring package with a starting price of around $250,000. In the middle tier, smaller monitoring solutions can be had for approximately $20,000. Some of these systems only permit inspection of devices on a local basis. Others permit a technician to inspect geographically diverse installations from a central console. However, all of these solutions are expensive to implement and complex and difficult to maintain and train personnel to use them.

As a result, small to medium companies having small to medium networks are left in the position of requiring a means to monitor and maintain their computer network equipment from failing while not having the resources to afford the high-priced solutions currently available. Many firms cannot afford a high-end solution or simply do not have the time and resources to train their IT personnel to learn and use complex systems. Instead, the common monitoring method in many such companies is user complains to the IT manager to indicate when a problem has occurred. The idea is that someone in the organization will notice a failure and call for repairs before damage can be done. The reality, however, is that most IT managers have suffered some form of server room damage from excess heat or other physical phenomenon or simply just failure.

This is especially true for companies having multiple server rooms and that have concerns about routine access to each of these rooms. For example, most IT managers would like some form of remote access for determining the status of a server room. Additionally, concerns exist with current solutions regarding the manpower intensiveness of these solutions. Most network monitoring solutions can consume a full- or part-time employee. The financial justification for these systems is, therefore, difficult because network equipment typically fails yearly, or on a disaster basis, and the cost of recovery is seen as less than that of maintaining a full-time employee to routinely monitor the equipment.

Similar concerns exist for monitoring rack-mounted components such that individual components within a rack can be monitored remotely. Also, current monitoring solutions do not provide for video imaging of remote server locations over a network. Computer equipment is typically placed in server rooms for two reasons: security and environmental control. Remote video imaging of a server room over a network can provide for maintaining security of the equipment despite the lack of a physical presence on site.

A typical computer room can house hundreds of devices, ranging from expensive server grade computers to bridges, routers, uninterruptable power supplies and telephone equipment. A server room's environment requires monitoring because out of limit environmental variables can eventually affect the equipment in the room. For example, high temperatures, humidity (for example, from water

leaks), or lack of air flow can detrimentally affect the equipment. Similarly, alarms, such as smoke and fire alarms, or the status of room openings, are important to determine. While the expense of replacing server room components if they fail is great, currently existing monitoring solutions are not cost effective for smaller-sized companies to implement despite the potential costs of such losses.

SUMMARY OF THE INVENTION

Therefore, a need exists for a method and system for monitoring computer networks and equipment that can fit into different levels of information technology ("IT") management, from very large companies with large network operation centers and deployed worldwide networks, to small companies with one internet server.

A further need exists for a computer network and equipment monitoring method and system that can be implemented in a small space, is simple to install, maintain and manage, and is reliable. Such a system can be configured with no moving parts, such as the keyboard, disk drives or monitors of conventional computer systems.

An even further need exists for a computer network and equipment monitoring method and system that can provide access and control through a global network such as the internet and that are capable of processing HTTP, HTML, MIME, TeleNet, TCP/IP and SNMP, standards.

A still further need exists for a computer network and equipment monitoring method and system that can provide a video image of a room upon the occurrence of a pre-set condition, such as a door opening.

Still further, a need exists for a computer network and equipment monitoring method and system that can perform continuous computer network monitoring, monitoring of the environmental conditions of a computer room, and an evaluation of individual components, and automatically provide a report in the event of an out-of-limit condition. Such a system and method should be able to determine the power status of a device, use SNMP, Bios API, or Windows NT (or similar operating systems) to determine accessory conditions, assemble a complete report, and send email or pager messages on out-of-limit conditions.

An even further need exists for a computer network and equipment monitoring method and system that can communicate to personnel monitoring the system via the internet through, for example, an Ethernet 10-base-T Category 3 or Category 5 wire, or through an optional dial-up telephone line for network down conditions.

A still further need exists for a computer network and equipment monitoring method and system that can measure the physical conditions of a server room, such as room temperature, humidity, and/or air flow, and detect whether a smoke alarm has gone off.

Furthermore, a need exists for a computer network and equipment monitoring method and system that can report equipment or environmental conditions via the internet through a Web page, email or through a pager or a telephone call.

A still further need exists for a computer network and equipment monitoring method and system that can provide a downloadable memory function to make adding or changing functionality simple. IT managers can thus modify or even invent tasks for the system. Administration can be via straightforward HTML tables requiring no training.

A further need exists for a computer network and equipment monitoring method and system that can provide a micro web-server powered through an Ethernet cable, thus eliminating the need for the micro web server to have a wall-supplied power source.

Moreover, a need exists for a computer network and equipment monitoring system and method with the ability to control an external, high-voltage load from either a remote or local location.

In accordance with the present invention, a computer network and equipment monitoring method and system are provided that substantially eliminate or reduce disadvantages and problems associated with previously developed systems and methods for monitoring computer networks and equipment.

More specifically, the present invention provides a method and system for monitoring a space and its contents over a network. The system can include an embedded microprocessor, such as Java microprocessor, to provide processing and network connectivity capability, and sensors to detect physical parameters associated with the space. The sensors can generate one or more sensor signals representative of the detected physical parameters. An analog-to-digital converter can convert the sensor signals to a digital format and can provide corresponding digital signals to the microprocessor.

The system further includes instructions for processing the sensor signals and corresponding digital signals. An alarm signal can be generated when any of the physical parameters exceeds a corresponding threshold value. The system of the present invention can have at least one input/output port for communicating with the network and one or more memory modules for storing system data. The system of this invention can have a network-based interface for providing programming instructions to the microprocessor and for receiving monitoring status and alarm information from the system. The interface can be an HTML interface. A power source provides power to the system.

The present invention provides a technical advantage of a computer network and equipment monitoring method and system that that can be implemented in a small space, is simple to install, maintain and manage, and is reliable.

A further technical advantage of the present invention is its ability to provide access and control through a global network such as the internet and the capability to process HTTP, HTML, MIME, and SNMP standards.

An even further technical advantage of the present invention is the ability to provide a video image of a room upon the occurrence of a pre-set condition, such as a door opening or whenever the website is addressed.

Still further, a technical advantage of the present invention is the ability to perform continuous computer network monitoring, to monitor the environmental conditions of a computer room, and to evaluate individual network components and automatically provide a report in the event of an out-of-limit condition.

A still further technical advantage provided by the present invention is the ability to communicate with personnel monitoring the system via the internet or an intranet.

An even further technical advantage of the present invention is the ability to report equipment or environmental conditions via the internet through a Web page, email or through a pager or a telephone call.

A still further a technical advantage of this invention is a downloadable memory function to make adding or changing functionality simple.

Still further, a technical advantage provided this invention is a micro web-server powered through an Ethernet cable, thus eliminating the need for the micro web server to have a wall-supplied power source.

Moreover, a technical advantage of the present invention is a computer network and equipment monitoring system and method with the ability to control an external load from either a remote or local location.

It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the invention as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and the advantages thereof, reference is now made to the following description taken in conjunction with the accompanying drawings in which like reference numerals indicate like features and wherein:

FIGURE 1 shows a typical server room layout that can be monitored using the method and system of the present invention;

FIGURE 2 is a conceptual diagram showing a typical installation of an embodiment of the system of the present invention;

FIGURE 3 illustrates the capabilities of one embodiment of the computer network and equipment monitoring system of the present invention;

FIGURE 4 illustrates the capabilities of another embodiment of the method and system of the present invention;

FIGURE 5 illustrates the capabilities of another embodiment of the method and system of the present invention;

FIGURE 6 illustrates another embodiment of the computer network and equipment monitoring method and system of the present invention;

FIGURE 7 is a conceptual block diagram of an embodiment of the computer network and equipment monitoring system of the present invention;

FIGURE 8 is a simplified box diagram of the architecture of the embodiment of the present invention shown in FIGURE 6;

FIGURE 9 is a circuit schematic of humidity sensor 52 of FIGURE 7;

FIGURE 10 is a circuit diagram of air flow sensor 54 of FIGURE 7;

FIGURE 11 shows the physical layout of various embodiments of the present invention;

FIGUREs 12A, 12B, 12C, and 12D show various views of the sheet metal housing of an embodiment of the present invention;

FIGURES 13A, 13B and 13C show front, top, and side views, respectively, of the sheet metal housing of an embodiment of the present invention;

FIGURE 14 is a top level flow chart diagramming the operation of an embodiment of the computer network and equipment monitoring method of the present invention;

FIGURE 14A represents a flow chart of the process alarm conditions of the present invention.

FIGURE 15 is a flow chart diagramming the initialization process of the monitoring method of this invention shown in FIGURE 14;

FIGURE 16 is a flow chart diagramming the steps of the method of this invention for retrieving configuration settings;

FIGURE 17 shows a typical HTML response to a status request as provided by the method and system of this invention;

FIGURE 18 is a flow chart diagramming the response of the system and method of this invention to an HTTP request;

FIGURE 19 is a block diagram illustrating the signal processing steps of the method of this invention;

FIGURE 20 is a screen shot of a typical web page generated using the monitoring system and method of the present invention;

FIGUREs 21A and 21B show a typical alarm email and scheduled report email generated using the method and system of the present invention; and

FIGURE 22 represents a flow chart of the system operation of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Preferred embodiments of the present invention are illustrated in the FIGUREs, like numerals being used to refer to like and corresponding parts of the various drawings.

The method and system of the present invention can provide a simple, reliable, easy to manage and low-cost means for monitoring a network and the physical environment housing the network. Various embodiments of the present invention can provide one or all of physical environment monitoring, monitoring of individual component parts, video imaging of the physical space housing a server system, internet or Intranet connectivity and telephone-line notification. The method and system of the present invention can be implemented in data networks of very large companies with large network operation centers and deployed worldwide networks, to small companies with one internet server or a single computer room. In particular, the low cost, low maintenance, internet connectivity, and ease of use of the method and system of the present invention make it ideally suited for the currently under-served smaller network market.

FIGURE 1 shows a typical server room layout that can be monitored using the method and system of the present invention. Server room 10 includes racks 12, which can hold different types of devices ranging from expensive server-grade computing units to bridges, routers, uninterruptable power supplies, and telephone equipment. Communications lines to connect to the internet and to a telephone system can connect into racks 12. Typically, a heating, ventilation and air conditioning system 14 provides recirculation of cooled air through server room 10 and can be controlled by thermostat 18. Server room 10 can also include a smoke alarm 16 to indicate the presence of a fire or smoking equipment. Different embodiments of the system of the present invention can be used to monitor server room 10 by being placed, for example, on wall 20 in a position to monitor the contents of server room 10.

FIGURE 2 is a conceptual diagram showing a typical installation of an embodiment of the system of the present invention. Climate bot 28, comprising one embodiment of the method and system of the present invention, can connect via a standard ethernet connection to bridge router 26. Ethernet connection to bridge router 26 can be an RJ45 to category 5 network wiring connector. Company web server 30 is connected to bridge router 26 and, through bridge router 26, can be connected to an internal client 24 on a company intranet or to an external client 22 via the internet. External client 22 can connect to climate bot 28 via a dial-up internet connection or other internet connection to obtain the status of server room 10 monitored parameters. In a similar manner, internal client 24 can access climate bot 28 VIA an internal company intranet connection through bridge router 26. FIGURE 2 illustrates the local and remote access capabilities of the method and system of the present invention implemented as climate bot 28.

Many modern computers and computer peripheral equipment have the capability to permit monitoring of various system parameters, such as the on/off status of fans, processor temperatures,

various system voltages, and other system parameters. With the appropriate software and communications links, such systems can be queried for these various parameters. The method and system of the present invention can perform these monitoring functions. The system of the present invention can comprise a small, low-cost, self-contained, simple-to-install unit made from industrial construction materials. Various embodiments of the present invention can provide various levels of monitoring, notification, and video imaging. The embodiments of the present invention can be wall-mounted within server room 10 of FIGURE 1 in a position to both monitor the environmental parameters of server room 10 and to connect to a company's computer network to monitor various parameters of the computer network.

The embodiments of the present invention can comprise a complete and self-contained "micro" web-server with its own URL and static IP address on the internet, and can connect to a company's network, and through that computer network to the internet, via a standard connector such as an Ethernet connector. A unit comprising the system of the present invention can have its own worldwide web address and deliver a web page to users accessing the unit. The various embodiments of the present invention can be HTML compliant, provide email and/or phone notification, and essentially comprise an internet site.

FIGURE 3 illustrates the capabilities of one embodiment of the computer network and equipment monitoring system of the present invention. Climate bot 30 of FIGURE 3 can provide continual monitoring of a server room 10's environmental parameters. For example, climate bot 30 can provide continuous monitoring of temperature, humidity, air flow, and the presence of smoke within server room 10. Climate bot 30 can report the status of the parameters that it is monitoring via a web page, email, or paging. Internet connection 32 can connect climate bot 30 directly to the internet or to another computer network and through that computer network to the internet. A user can set alarm points for the parameters monitored by climate bot 30 using a simple HTML web page interface.

Climate bot 30 of FIGURE 3 can be configured as only an environmental monitoring system. However, climate bot 30 can be upgraded to include agent ("bot") functionality. Agents are software objects that can be used to investigate and query individual components of the computer network to determine their status and some physical parameters.

FIGURE 4 illustrates the capabilities of another embodiment of the computer network and equipment monitoring method and system of the present invention. Video climate bot 34 incorporates a video imaging system, such as a CMOS imager, to provide images of server room 10 Video climate bot 34 can be mounted on wall 20 so as to provide an unobstructed view of the entrance to server room 10, or any other portion of server room 10. Video climate bot 34 can have all of the same functionality of climate bot 30 of FIGURE 3, but can also provide video imaging circuitry and circuitry for sensing an external influence, such as the opening of door 36. A sensor 38 can monitor

door 36 and provide a signal to video climate bot 34 upon, for example, the opening of door 36. Sensor 38 can be any type of sensor, such as a magnetic switch, that can provide a signal upon the occurrence of a preset condition. Sensor 38 can be connected to video climate bot 34 by hard wiring, or through a wireless interface.

In one embodiment of the present invention, video climate bot 34 can be set to receive an input signal from sensor 38 indicating that door 36 has been opened. Video climate bot 36 can be configured to wait a pre-set amount of time (for example, one second) following the opening of door 36 and take a video image of server room 10. The video image can be transmitted to a system administrator to indicate the presence of an external influence, such as a person, entering server room 10. Video climate bot 34 can thus be used as an additional security measure and record-keeping device to track personnel access into server room 10. Video climate bot 34 and sensor 38 can also be used to indicate the presence of other external influences beyond personnel access to server room 10.

Video climate bot 34 can be slightly larger than climate bot 30 of FIGURE 3 to accommodate a video imaging system. Each time that a web page maintained by video climate bot 34 is accessed, a new image can be captured and transmitted to the user. Video climate bot 34 can also provide streaming video or truce frame (still frame) over to the user.

Climate bot 30 of FIGURE 3 and video climate bot 34 of FIGURE 4 can both provide information relating to the various parameters they are monitoring through a simple HTML interface. Both units can be accessed, configured, and maintained via the internet using standard HTML. Unlike in prior art computer network monitoring systems, extensive personnel training is therefore not required. Video climate bot 34 can provide the administrator of a large network system with various geographically distinct server rooms 10 with the ability to tour the server rooms remotely, via the internet or an intranet, and be able to see an image of each of those server rooms. The system administrator can likewise monitor the environmental conditions in each of the server rooms quickly and efficiently, without having to physically visit each room.

FIGURE 5 illustrates the capabilities of another embodiment of the computer network and equipment monitoring method and system of the present invention. Net bot 40 can have the same functionality as video climate bot 34 of FIGURE 4 and can additionally provide the capability to detect a power failure or loss of an IP connection within a computer network, and the capability to provide dial-up telephone notification of the occurrence of these conditions. Net bot 40 can provide agents to monitor and continuously detect if an internet connection is active and if the main power grid serving the network is on. If an internet connection, or main power, is lost, net bot 40 can dial out via telephone connection 42 to inform a system administrator of the loss of power or loss of the internet protocol connection. Dial-up telephone notification via telephone connection 42 can serve as a failsafe in the event that net bot 40 cannot communicate with the system administrator via the internet through an email. As with climate bot 30 of FIGURE 3 and video climate bot 34 of

FIGURE 4, net bot 40 of FIGURE 5 can be upgraded easily to provide agent functionality to monitor the various parameters of a computer network.

FIGURE 6 illustrates another embodiment of the computer network and equipment monitoring method and system of the present invention. Net bot 40 of FIGURE 6 can have SNMP, DMI and NT access for internal server monitoring. Like enterprise-class network monitors, net bot 40 can periodically check for SNMP traps, Windows NT traps, and BIOS alerts, and can notify the system administrator of their occurrence. Common functions of net bot 40 can include checking the on/off status of both CPU fans and other system fans, CPU temperature checking, and checking of the conditions of various disk drives. Net bot 40 can support various protocols, including SNMP (simple network message protocol). Net bot 40 can launch software agents that can determine the operating condition of system routers, bridges, uninterruptable power supplies, etc. If the agents find a stuck disk, for example, on a server, they will log it as a fault. When a fault is detected, agents of net bot 40 can return that condition to net bot 40 in java language, and net bot 40 can generate an email message reporting the malfunction. Net bot 40 can be configured to maintain an email list of all personnel the system administrator wants net bot 40 to notify. Net bot 40 can also be configured to, after waiting a certain amount of time following email notification, page the system administrator or other personnel.

Beyond receiving notification via email of a fault, a system administrator, or other user, can obtain real-time reports of environmental conditions and equipment conditions in a server room via an internet connection to net bot 40. Additionally, if, like video climate bot 34, the embodiment of the present invention being used by a system administrator provides video, a current video image of the monitored server room 10 can also be viewed via the internet. A system administrator can configure net bot 40, climate bot 30, or video climate bot 34 to provide only the information the system administrator is interested in receiving. In this way, the interface of the embodiments of this invention can be kept as simple or as complex as a system administrator requires. Any of the embodiments of the present invention can be upgraded via software that can be downloaded from the internet.

Another embodiment of the computer network and equipment monitoring method and system of the present invention can be mounted within a component rack, such as rack 12 of FIGURE 1. This "rack bot" can provide the same functionality as climate bot 30, video climate both 34, or net bot 40, but in a smaller package that can be mounted internal to a rack 12. In this way, individual components within a rack 12 can be monitored and a web page provided for each component monitored by a rack bot. One use for a rack bot according to the teachings of this invention could be, for example, to monitor individual components of companies or individuals that lease out space within another company's rack for their own servers or other components. Using a rack bot, the individual or company renting space within someone else's rack could independently monitor their

equipment. Rack bots can be mounted inside of a rack using, for example, Velcro or some other attachment method.

Each of the embodiments of the computer network and equipment monitoring method and system of the present invention described above can be stand-alone units configured and maintained by a system administrator. However, they can also be easily incorporated into an existing monitoring system to complement or augment that system. This is possible because the embodiments of the present invention can be object properties and can be accessed as such.

The embodiments of the present invention shown in FIGUREs 5 and 6 illustrate the capability of this invention to launch agents or bots from a satellite platform. Typically, agents for monitoring a computer system's performance are resident on the system. These agents typically can be made to perform their function and then can be placed in a "sleep" mode. Prior art platforms thus typically invoke agents and receive information from agents on the platform itself. The embodiments of the present invention, in contrast, can invoke agents resident on a system, such as a computer network, from a remote satellite position. They can invoke the system's own agents remotely, receive information from the agents, and pass the information to a user. Furthermore, net bot 40 of the present invention and other embodiments of the present invention, can be upgraded with support for new agents to query new equipment that is added to the network. In this way, net bot 40 and the other embodiments of the present invention can be kept current and can be used to monitor equipment that is newly added to an existing computer network.

FIGURE 7 is a conceptual block diagram of an embodiment of the computer network and equipment monitoring system of the present invention. Circuit 50 contains video imager 52 for receiving and capturing images of the monitored server room or other space, temperature sensor 60 for sensing temperature within the space, humidity sensor 62 for monitoring relative humidity, and air flow sensor 54 for monitoring the status of cooling air flow within the monitored space. This sensor circuitry also can process environmental information received to help eliminate noise and make the information more useful to microprocessor 72. Analog amplifier 58, image logic module 56, and image buffer 64 combine to receive, translate, process and forward the images captured by video imager 52 to the system web site. Analog-to-digital converter 66 converts the analog signals received from the various sensors to their digital equivalent for microprocessor 72.

Microprocessor 72 is the central circuit element with which all other circuit components interface. Microprocessor 72 can be a Dallas Semiconductor 80C390 microcontroller. Memory modules 68 and 70 are used to store both persistent and temporary information required by the system. Line interface 76 and internet interface 74 provide the interface between microprocessor 72, telephone module 80 and ethernet RJ45 connector 82. Analog-to-digital converter 66 converts the analog signals received from the various sensors to their digital equivalent for microprocessor 72.

Five-volt power supply 78 can receive and transform electrical power from a wall-mounted receptacle to power circuit 50. Humidity sensor 52 and air flow sensor 54 are described in more detail below.

FIGURE 8 is a simplified box diagram of the architecture of the embodiment of the present invention shown in FIGURE 6. Sensors 54, 60, 62, 84, and 86 interface to the analog-to-digital converter 66 which converts the signals for use by the microprocessor.

The solid state imager 52 is a VLSI Vision 5300 CMOS imager and incorporates the auto-imaging algorithms 56. The algorithms include gamma correction and anti-blooming and are included because any solid-state cameras do not incorporate these algorithms in hardware, so if there is a need to implement these in software if another camera is to be chosen. Buffer 64 and Parallel Interface 65 provide the necessary logic to interface directly to the CPU's data bus.

MHDY Clock 92 is a battery powered real-time clock that maintains a clock for the system that provides time in hours and minutes as well as months, days and years. The clock used is a Dallas Semiconductor DS1315.

The 5VDC power supply 78 is generated from a typical wall supply that converts 120V to a regulated 5V. The power fail detector 88 can be integrated as part of the power supply or detected from an external source such as an uninterruptable power supply. This sensor detects the failure of the supply from the utility company and provides a means of switching the device to battery power 90 as well as notifying the CPU of the power failure.

The SNMP client 106 implements the common functions necessary to query the status of external devices such as routers, bridges, and uninterruptable power supplies. The necessary functions for SNMP clients is defined by the IETF.

The email generator 104 is a standard SMTP client that generates MIME compliant email. Like SNMP, the standards for this type of program is documented in a number of documents issued by the IETF.

The alarm rules 102 are the set of conditions specified by the user of the device. When any of these conditions is true, the ClimateBot engine 100 will generate an email via the email generator 104. This email will be sent to a specified set of recipients.

The ClimateBot Engine 100 provides the integration of all the other parts of the device. It generates the HTML pages using information provided by sensors 54, 60, 62, 84, & 86, the camera, and the SNMP client 106. It also monitors the alarm rules 102 for error conditions.

The ClimateBot engine communicates via one of two means. It can communicate using a standard 10BaseT ethernet 94 or it can communicate using a telephone lien interface 112. The choice of communications channel does not change how the ClimateBot engine communicates with the outside world. The device still routes its messages through a TCP/IP stack 96 which in turn routes the message either to the ethernet driver 94 or through the PPP driver 108, serial interface 100 and on to

the telephone module 112. The PPP (point-to-point) driver 108 is a standard means of using a communicating over a serial link reliably. It is well documented in IETF standards.

The family of NetBotz, ClimateBots may be powered by using power existing on the ethernet cable either in the form of data or power on the cable. The data signals will be received and averaged to supply a continual source of voltage and current to the Netbot or ClimateBot device. Thus eliminating the need for external power supplies. The device shall receive the data and use an appropriate amount of power from ethernet data signal or power signal such as to not disturb the signaling capacity of the line only to use the excess capacity of the signal lines.

FIGURE 9 is a circuit schematic of humidity sensor 52 of FIGURE 7. Humidity sensor 52 is used to sense the relative humidity of the air within a space. Humidity sensor 52 includes relative humidity sensor chip 202, which can consist of a ceramic plate that shrinks or expands with changes in relative humidity. The shrinking and expanding generates an electrical signal proportional to relative humidity. Humidity sensor 52 operates under well-understood principles of electrical circuitry to provide an indication of relative humidity. A person of average skill in the art can understand and reproduce the functionality of humidity sensor 52.

Humidity sensor 52 is comprised of five parts: an oscillator, a lowpass filter, humidity sensor chip 52, and two peak detectors. The oscillator subcircuit can consist of resistors r3, r5, r7, and r15, capacitor c6, and op-amp U1B. This subcircuit produces a square-wave with a nominal frequency of 1khz. The square-wave signal is lowpass filtered using a two-stage lowpass filter. The first stage consists of resistor r16 and capacitor c4. This is a passive filter, so the output is slightly attenuated. The second stage of the filter has some gain to make up for the attenuation of the first stage. The second stage of the lowpass filter consists of resistors r10, r17, capacitor c7, and op-amp U1A. This lowpass filter provides a waveform shaping function. The output of the lowpass filter approximates a sinusoidal waveform.

The output of the lowpass filter passes directly to humidity sensor chip 202 as well as to a first peak detector. Humidity sensor chip 202 can be a Figaro Engineering NH-2 humidity sensor. Humidity sensor chip 202 attenuates the amplitude of the input sinusoid waveform based on the relative humidity. The output of humidity sensor chip 202 passes to the second peak detector.

The first peak detector, consisting of diode D2, capacitor C3, and resistor R19, provides an estimate of the amplitude of the humidity sensor input. Likewise, the second peak detector, consisting of diode D1, capacitor C1, and resistor R1, estimates the amplitude of the humidity sensor output. The relative humidity is determined by computing the ratio of the output amplitude to the input amplitude.

FIGURE 10 is a circuit diagram illustrating the air flow sensor 54 of FIGURE 7. Air flow sensor 54 essentially acts as an air-on/air-off indicator. Air flow sensor 54 is comprised of a "hot wire" anemometer circuit and a differential amplifier.

The anemometer circuit can consist of resistors R6 and R9, potentiometer R8, and two thermistors 302 and 304. Thermistors 302 and 304 vary resistance with temperature. The anemometer components can be placed in a classic 'wheatstone bridge' configuration. Each leg of the bridge contains one of the resistors and one of the thermistors. One of the legs also includes potentiometer 306.

Thermistor 302 is mounted near the opening of, for example, net bot 40 and is exposed to the environment being monitored. Thermistor 304 should be mounted such that it is shielded from the air flow, such as within the outer casing of net bot 40.

When no air flow is present in the space being monitored, both legs of the bridge will have equal resistance except for a small difference due to component tolerances. Potentiometer 306 can be used to compensate for this difference. When air flow is present, thermistor 302 will change its resistance because the air flow changes the temperature at thermistor 302. Thermistor 304 will not change because no air flow reaches it.

The voltage across each of thermistors 302 and 304 passes to the inputs of the differential amplifier. The differential amplifier amplifies and filters any difference between the thermistor 302 and 304 voltages. The filter operation limits the effect of any fast changes in temperature that would not be due to air flow. The amplified differential voltage provides a signal indicative of air flow.

Air flow sensor 54 can be used to inform a system administrator if the air conditioner blowers have failed in a given space. Typically, air registers in a server room blow air across the ceiling and down the room walls, so the location of net bot 40 on a wall is a good location to determine whether air flow is on or off. Air flow sensor 54 need not be calibrated to indicate flow in any given units, but can be if desired. Neither air flow sensor 54 nor humidity sensor 52 need be recalibrated and hence are essentially maintenance-free components.

Returning now to FIGURE 7, temperature sensor 60 can be a standard off-the-shelf temperature detector and is typically accurate to within a degree. Smoke detector 84 can be a microphone with a notch filter. The notch filter of smoke detector 84 can be calibrated to detect only frequencies typically associated with smoke detector alarms in buildings. All other sound frequencies can be excluded, and smoke detector 84 will only generate an alarm condition signal if the frequencies associated with a smoke detector alarm are detected. Smoke detector 84's functionality is especially useful in applications where smoke detector alarms are self-contained, battery-operated units. Configuration of smoke detector 84 eliminates the need for running wiring between a smoke detector alarm and any embodiment of the computer network and equipment monitoring system of the present invention. Sensor 86 of FIGURE 8 can be an external sensor, such as a magnetic switch connected to a door leading into a server room, and can provide a signal when the door is opened.

FIGURE 11 shows some of the embodiments of the present invention as described above. Climate bot 30 is shown with four LEDs 252. LEDs 252 can indicate, for example, that temperature

and humidity are within limits, or can be used as a "heartbeat" indicating that the unit has power and is operational. A front view of climate bot 34 is also shown with four LEDs 252 and video imager 254. One variation of net bot 40 is shown without LEDs 252, but having video imager 254. Rack bot 250 is shown with video imager 254. Although only a few embodiments of this invention are shown in FIGURE 11, various combinations that have not been described are possible. Features from one of the embodiments of the present invention can be combined with the features of another embodiment to form a new embodiment.

FIGUREs 12A, 12B, 12C, 12D show various views of the sheet metal housing of, for example, climate bot 30. Although particular dimensions and locations of slots, perforations, notches and indentations are shown, these are illustrative only and various other dimensions and combinations of such slots, perforations, notches and indentations are possible. FIGURE 12A is a front view of climate bot 30's housing, FIGURE 12B a top view, and FIGURE 12C a side view. FIGURE 12D shows a full frontal view of the housing with the accompanying lettering that can be placed on the surface of the housing. FIGURE 12D also shows the spaces on the housing that can be made available to record the URL address 260 for a given unit, as well as the email address 262 that can be programmed into the unit for email alerts.

FIGURES 13A, 13B and 13C show front, top, and side views, respectively, of the sheet metal housing of, for example, video climate bot 34 of FIGURE 4. As in FIGURE 12, the views in FIGURE 13 are illustrative only, and the dimensions shown can be changed to fit different embodiments of the computer network and equipment monitoring system of the present invention. FIGURES 13A shows video climate bot 34's sheet metal housing with opening 270 to accommodate video imager 254.

An embodiment of the computer network and equipment monitoring method and system of the present invention incorporating micro web-server technology and video imaging technology as described above could be used, for example, in an on-line auction type environment. This could allow, for instance, the placing of goods for auction on a site such as eBay by creating a link to the web site of a micro-web server according to the teachings of the present invention. Someone visiting the auction site and wishing to bid on the offered goods could click on the link and get a real-time image of the goods offered for sale. This can eliminate the problems of prior art methods that required someone offering goods for auction on line to take a digital picture, or digitally scan a regular picture, store the resulting image on their home page or local site, and hot link to the stored image.

This embodiment of the present invention can be as simple as the self-contained micro web server described above with a digital camera and an ethernet connection to the internet. Real-time video images could thus be sent to on-line users to provide an image of goods offered for sale or that are to be monitored. In this way, a very small computer of limited memory can be used as a net-cam

URL generator to provide essentially real-time images via creation of a unique web site that can be accessed remotely. This method requires the use of an embedding process for response generation, whereby a user clicking onto the web site causes a still image to be captured by the camera of this embodiment of the present invention and forwarded to him or her.

Returning now to FIGURE 7, microprocessor 72 of FIGURE 7 can be a TINI (tiny internet interface), a virtual machine developed and sold by Dallas Semiconductor as described above. Dallas Semiconductor's TINI is a compact circuit board or chip set that incorporates the latest in low-cost embedded java technology. Using TINI, it is possible to develop java applications quickly and easily to provide an internet or intranet interface for the system of the present invention. Combined with a simple web server application, microprocessor 72 can become a very small Java web server. In this way, the machinery and the network can be melded into a single entity. The system of the present invention can thus talk to a computer network by use of a specialized java data language and the improved processing capabilities provided by microprocessor 72 while maintaining low cost.

The high level of integration incorporated into microprocessor 72 allows software developers to write efficient, I/O-intensive Java applications. In typical applications, microprocessor 72 can control and monitor attached equipment and transfer collected control and status information over a computer network as described above. Microprocessor 72's three-chip set consists of a microcontroller, flash memory containing the firmware, and an ethernet controller. The microcontroller integrates serial, parallel 1-wire, and controller area network (CAN) ports, with extra pins for controlling optional devices such as relays and indicator LEDs. Microprocessor 72 can address up to four megabytes of RAM and 512 kilobytes flash memory. An integrated real-time clock enables time stamping and time-dependent functionality. For security sensitive applications, a physically secured coprocessor with advanced cryptographic capabilities can be made available.

Microprocessor 72 of the present invention is optimized to accommodate the embedded java environment. The microcontroller supports 24-bit addressing and 8/32-bit CPU/ALU and high clock rates of approximately 60MHz and other java enhancements. Microprocessor 72's I/O ports include Ethernet 10 base T interface, dual 1-wire net interface, a CAN interface, a dual serial port (one RS232 level and one +5V level), an I^2C port, and an expansion bus allowing nearly unlimited parallel ports and miscellaneous digital and analog I/Os. The software platform on which microprocessor 72 runs is embedded Java implemented in firmware that is programmed in the flash memory and can be upgraded as necessary.

Microprocessor 72 includes a java virtual machine (VM/API), a multi-tasking, real-time operating system (RTOS), and a TCP/IP networking stack. The java virtual machine on microprocessor 72 conforms to Sun's Embedded Java™ platform. Various Java packages can be embedded in microprocessor 72's flash memory. An additional advantage of using a java processor is

that the system of the present invention can eventually be migrated to cheaper processors as they become available, without having to re-write the core software.

A further advantage of the computer network and equipment monitoring method and system of the present invention is that it can be powered directly through an Ethernet connector as an alternative to wall-mounted transformer. Typically, an Ethernet cable carries a large voltage in order to move data between network components. The voltage generated to move data along an Ethernet cable is generally much greater than is necessary, and the excess generally resolves itself as heat in the network inductors. The computer network and equipment monitoring method and system of the present invention can use the excess voltage and current flowing through an Ethernet cable to power itself. For example, the excess current generated by the excess voltage in the ethernet cable can be used to charge a rechargeable battery on a wall-mounted unit. Additionally, microprocessor 72 can be placed into a stand-by mode to conserve power.

The present invention is fully programmable in an HTML format using HTML forms. Programming can be performed locally or remotely through a web interface. The various monitored parameters can be configured through a web interface, as can the alarm setpoints. Unlike in current network management systems and methods, network management can be accomplished through a simple and easy-to-understand web interface.

The embodiments of the present invention can be configured to, locally or remotely, operate an external load through an internet or intranet interface in response to a preset condition or in response to a command from a system administrator. For example, auxiliary A/C units could be set to turn on when the room temperature reaches a pre-set limit. The present invention can include one or more binary (on-off) outputs connected to one or more relays that can control an external load or loads. The loads can be high voltage loads.

An RF (radio frequency) output, or other wireless output, can also be incorporated into any of the embodiments of the present invention to allow a wireless call to such an external load. Furthermore, it is possible to load a 64-bit encoded chip onto the circuit board of any of the embodiments of the present invention to provide encryption and password security. Privacy protection in the form of a private key and a public key can be provided. The present invention can also include additional outputs to provide audible alarms or for interfacing to other proprietary monitoring systems.

The embodiments of the present invention can provide a low-cost, reliable, self-contained web server using industrial-grade embedded processes and commercial-grade semiconductors. The present invention can be manufactured with no moving parts, increasing its reliability. The present invention can also, using a central data collection java program, automatically scan and store multiple sites for an IT manager to allow the IT manager to avoid looking through emails from past condition reports or trend analysis.

The present invention searches for equipment that is either on or off line and uses the static IP address, among other identifiers, to address and locate the device. The search can provide the IT manager with information, such as device availability, capacity, and inventory, as well as gathering information for the analysis and creation of trend lines. The trend lines may be used by the IT manager to perform maintenance or to schedule replacement of failing or suspect devices in an orderly and efficient manner.

It should be noted that the present invention is self-contained and does not need to be connected to or integrated with the users system or cpu. The present invention can be linked up with one or more of the users system via standalones, laptops or any other cpu to take advantage of any additional functionality that those systems might provide, although it is not necessary for the implementation and operation of the present invention.

The web interface of the computer network and equipment monitoring method and system of the present invention provides the ability to manage agents from any web browser, from across the room or across the globe. The self-contained web servers in each embodiment of the present invention can create their own web site. The embedded web server of this invention can thus be managed and configured from a standard web browser. End users therefore need not install new software on their systems or train their staff on how to use the system. A monitored space's condition can thus be quickly access via a web browser.

The various embodiments of the present invention can report static and dynamic system-critical events logged by a system's files and can provide an integrated user interface that can be launched from IT enterprise management (ITEM) applications. Various embodiments can provide alert redirection to stations and management consoles of other monitoring systems, such as HP Open View. The present invention can also provide management of on-equipment display devices such as local LCD panels. The present invention can also be DMI compliant and support SNMP traps. The various embodiments of the present invention can also support LM75/78/79 and other health devices, devices on ISA, SM Bus and 12C Bus and can provide DMI event generation on status changes.

The present invention can comprise a device having an embedded processor connected to a temperature sensor, humidity sensor and air flow sensor that can be programmed to report the values of these physical parameters via an HTML interface. The present invention can be configured to generate email messages and paging notification events when one or more parameters exceeds a user configurable threshold value. The system of the present invention can be configured via an HTML interface. Furthermore, the present invention can include an image capture device, such as a CMOS imager, or other digital camera. Thus configured, the present invention can further provide real-time images of a monitored space.

The present invention can store an image from the video imager in response to a binary (on/off) input when the binary input is active. The binary input can be provided by an external sensor

such as a magnetic door switch. Furthermore, the present invention can be programmed to continuously investigate the internal condition of numerous network devices through SNMP, DMI, and SMBIOS interfaces. The present invention can determine the status of fans, CPUs and other relevant components and include status information, along with the environmental parameters of the monitored space, to create a unified HTML or email report. A user can configure the system of the present invention via an HTML interface.

FIGUREs 14-19 are flow charts diagramming the operation of an embodiment of the method of the present invention. FIGURE 14 is a top level flow chart diagramming the operation of an embodiment of the computer network and equipment monitoring method and system of the present invention. At step 400, system initialization occurs. The initialization process can be run at power-up. The one-time setup of the processor, peripherals, and software can be performed at initialization.

The top-level of the program of the method of the present invention can consist of an infinite loop. Each time through the loop, the program can check for network messages. The program also contains a clock. This clock can be checked each time through the loop. When the clock reaches a certain time interval, such as a one-second interval shown in step 404 of FIGURE 14, the program can be configured to read the sensors, perform required calculations, and check for alarm conditions, as discussed below.

At step 402, the method of this invention continuously polls the Ethernet hardware to check for incoming network messages. When a network message arrives, the program can launch a new process and pass the received message to the new process. This new process can act on the message based on the message request.

At step 406, the method of this invention can read the temperature and all other channels of the analog-to-digital converter once per second, as determined at step 404. The program computes the temperature in degrees Fahrenheit, relative humidity in %, and air flow (on or off).

The method of the present invention can maintain a list of user-specified thresholds for each monitored quantity. At step 408, the method checks the sensor readings against the relevant thresholds to determine if an alarm condition exists. The method of this invention performs this check at a preset interval, as determined at step 404. The method of this invention can generate an email report when one of the sensors is outside its corresponding threshold value.

At step 408 the program checks for alarm conditions once per second, but can be set for other time periods, but only if the program hasn't recognized any alarm conditions in the past 5 minutes. This limiting condition prevents the recipients of the email reports that get generated from being inundated with one email per second. The program could just check for alarm conditions once every 5 minutes; but this would mean that up to 5 minutes could go by from the time an alarm condition occurs and the device actually recognizes the condition and tries to notify someone.

The program next checks the sensor readings against the stored threshold values. A temperature alarm occurs when the temperature reading is outside the range defined by the high and low temperature thresholds. Similarly, a humidity alarm occurs when the humidity readings is outside the range defined by the high and low humidity thresholds. An air flow alarm occurs when no air flow is detected for the specified period of time.

When an alarm condition occurs, the program then generates an email message consistent with the standards for email messages set forth by the IETF. An alarm message simply states the sensor causing the alarm and the current value of that sensor. The email message is then sent to the list of recipients that was specified in the administration form and stored in the configuration.

The program can also send the same email message to a digital pager or email-enabled cell phone. However, because the service providers of these communication devices often charge for each email message sent to the device, the program will only send a message to the designated pager address once per hour.

The device may also include software to check external devices such as routers, servers, or UPS's via the network. Such programs are referred to as 'crawlers' or 'bots'. If any of these bots have placed on the device; the program will periodically execute them. These programs will return the status of the external device and indicate if any component on the device has failed. If any component has failed, then an alarm email will be generated.

FIGURE 15 is a flow chart diagramming the initialization process of the monitoring method of this invention shown in FIGURE 14. At step 410, a file containing user-defined settings for the various parameters of the system of this invention is accessed to determine the appropriate system variables. Those variables can be read and set at system power-on.

At step 412, hardware peripherals are configured to operate as desired. This typically must be performed at power-up. In particular, the Ethernet controller chip is configured to interface with the microprocessor in 8 bit mode. The analog-to-digital converter is set to provide 16-bit results with inputs in the range 0-5V. Other system variables can also be configured.

The techniques used by the method of this invention to compute humidity and air flow require some digital signal processing calculations. These calculations require a number of buffers to store intermediate values. At step 414, the contents of these buffers are initialized to 0.

At step 416, the method of this invention creates a TCP socket on port 80. Software applications that interact with the worldwide web perform many of their transactions on TCP port 80. Because the system of this invention can behave as a server 'on the web,' a TCP socket on port 80 is necessary in some instances. The system of this invention will not be visible 'on the web' until this socket is created.

The method of this invention can retrieve configuration settings as shown in FIGURE 16. At step 418, a configuration file is read to determine the values of certain system variables. In order to

respond to network messages, the system of this invention needs to know a number of settings. At step 420, network variables are initialized as determined from the configuration file. For example, the system must know its IP address in order to receive messages. Similarly, the subnet mask and the gateway IP address of other devices are needed to properly route messages to them. To send email, the system of this invention must know the IP address of an SMTP (Simple Mail Transfer Protocol) server. An SMTP server is roughly the electronic equivalent of the US Postal Service's blue mailboxes. The other network related settings that the method and system of this invention can store are the network name of the system, the internet domain name in which the system is implemented, and the list of email addresses that will receive the alarm reports generated by the system.

Some of the information stored in the configuration file is only used as part of an HTML response to a request on TCP port 80. This information includes the system name, the physical location of the system, and the name of the person in charge of the system. A typical HTML response to a status request is shown in FIGURE 17.

Stored location 426 is shown in FIGURE 17. The remaining values are used in response to a request for administration data. These values include temperature 428, humidity 430, and air flow 432. Temperature can be provided in Celsius or Fahrenheit units. FIGURE 17 also includes email notification addresses 434 to which the report is sent.

Returning to FIGURE 16, at step 424 the method of this invention initializes the alarm thresholds for the monitored parameters. These user- specified thresholds can be maintained in the configuration file and can include high temperature, low temperature, high humidity, low humidity, and 'maximum air off time'. The 'maximum air off time' is the amount of time with no air flow the system will wait before the program declares a no air flow alarm.

FIGURE 18 is a flow chart diagramming the response of the system and method of this invention to an HTTP request. At step 440, the system determines if a request has been sent to TCP port 80. HTTP requests are typically in the form of "Method Filename Version". The 'Method' tells the system what operation to perform on the 'Filename'. The 'Version' tells the program what version of HTTP the requesting browser is using. This is all part of the HTTP standard that was drafted by the internet Engineering Task Force (IETF), the organization that controls internet standards.

At step 442, the method of this invention first looks at the 'filename' part of the request. The method will respond to requests for filenames "status" or "admin." If no filename is given, the method assumes the request is for the status. If a filename is given that is not a "status" request, then at step 444 the method of this invention determines if the request is an "admin" request.

If the request is a status file request, then at step 446 an HTML file is generated similar to that shown in FIGURE 17. At step 460, the file is sent as output to the user requesting the file.

At step 448, if the request is for the administration file, the method checks to see if the request came from an authorized user. If the request did not come from an authorized user, an HTML response indicating an error will be generated at step 452. Similarly, an error request will be generated if at step 444 the request is not for the admin file.

If the user is an authorized user, then at step 450 the method of this invention determines if the request 'method' is either 'get' or 'post.' If the request 'method' is 'get,' then at step 454 an HTML form is generated that includes entry fields for all the configuration settings previously mentioned, as well as a "submit" button. The user requesting the administration information can change whatever information he or she chooses and submit the information to the system. When the submit button is pressed, the browser (Netscape Navigator or internet Explorer, for example) can generate an HTTP 'post' request for the administration page and include with the request the values placed in each of the entry fields.

When a post request is received for the administration page, then at step 456 information that represents the values placed in the entry fields of the form is parsed off. The values placed in the entry fields can be matched to the corresponding variables in the program. These variables are updated and the new configuration is stored.

Once the configuration is stored and the program variables successfully updated, at step 458 an HTML response can be generated that displays the new settings. This response can then be sent to the user at step 460.

The system of the present invention can use a Dallas Semiconductor DS1820 temperature sensor. The temperature sensor provides microprocessor 72 with a number representing the temperature in 0.5C units. This number can be converted to both units of °C and °F. There are a number of other commercially available temperature sensors that can be used in the system of this invention.

The system of the present invention can include an analog-to-digital converter (ADC) 66, which can be a four-channel ADC. The circuitry for the humidity and air flow sensors is connected to the ADC 66. ADC 66 does not generate a conversion until it is directed to do so. The system of this invention can, for example, instruct ADC 66 to make a conversion once every second.

The circuitry comprising humidity sensor 62 can provide two signals to compute relative humidity. Two adjustments to these signals must be made before the humidity value can be computed. First, the signals are offset by 2.5 volts, so this value must be subtracted from both of the converted values. Second, the voltage drop lost across the diodes in the circuit must be added back to the converted values so that an accurate humidity value can be computed. The ratio of these two adjusted signals defines an index into a lookup table. The system determines the relative humidity by retrieving the value in the table at this index. This value represents the relative humidity as a percent.

The monitoring system of this invention can derive the presence or absence of air flow from a signal provided by the anemometer circuit. This derivation can be implemented by a series of signal processing steps. A block diagram of the signal processing steps is shown in FIGURE 19. First, the signal is highpass filtered at step 470 to remove slow variations in the signal that might be caused by time degradation of circuit elements or temperature changes that occur on the order of hours. The absolute value of the highpass filtered signal is taken at step 472 to remove negative signal swings. Circuit noise can cause a persistent signal to be present in the absolute value of the highpass filtered signal. This persistent signal can be negated by lowpass filtering at step 474, the absolute value of the highpass filtered signal and then subtracting the lowpass filtered signal from the absolute value signal at step 476. This resulting signal may falsely indicate air flow due to abrupt circuit disturbances or even humans walking past the device. To reduce the possibility of these false indications, the signal can be integrated at step 478. When the integrated signal exceeds a fixed threshold at step 486, the system can provide an indication that air flow is present.

The monitoring method and system of this invention can check for alarm conditions on a preset time interval. These checks can be set to occur only if an alarm condition has not occurred within a second preset time interval. This limiting condition can be used to prevent the recipients of the email reports that get generated by the system of this invention from being inundated with emails.

To determine if an alarm condition exists, the present invention can check the sensor readings against the stored threshold values. A temperature alarm can occur when the temperature reading is outside the range defined by the high and low temperature thresholds. Similarly, a humidity alarm can occur when the humidity readings is outside the range defined by the high and low humidity thresholds. An air flow alarm occurs when no air flow is detected for the specified period of time.

When an alarm condition occurs, the present invention can generate an email message consistent with the standards for email messages set forth by the IETF. An alarm message can simply state the sensor causing the alarm and the current value for that sensor. The email message can be sent to the list of recipients specified in the administration form and stored in the configuration.

The monitoring system of this invention can also send the same email message to a digital pager or email-enabled cell phone. However, because the service providers of these communication devices often charge for each email message sent to the device, the monitoring system of this invention can be configured to send a message to the designated pager address once per hour to limit expenses.

FIGURE 20 is a screen shot of a typical web page generated using the monitoring system and method of the present invention. Web page 400 from a typical web browser, such as Internet Explorer or Netscape Navigator, includes climate bot report 402, which can comprise table 404 listing the various measured parameters and their values, and table 406 listing the current alarm settings for those variables. Image 408 can be included using some embodiments of the present invention that

incorporate a video image to display a real-time image of the space being monitored. Additionally, destinations for alarm emails can be listed on web page 400. A system administrator can also designate additional information to be displayed on web page 400 for any of the embodiments of the present invention.

FIGUREs 21A and 21B show a typical alarm email and scheduled report email that might be sent out by the computer network and equipment monitoring method and system of the present invention. The emails can include the date, location, the identity of the micro-web server sending the email, whether any of the parameters being monitored are in or out of limits, and the current limit settings. Additional information can be specified by a user for inclusion in the email reports.

FIGURE 22 is a schematic diagram of the flow of the The device opens a TCP connection to the external device. The specific port may be specified by the manufacturer of the device or the specific protocol (SNMP, DMI, etc...) being used to communicate.

Query the device. This may be a standard SNMP query as defined by IETF standard for SNMP or it may be DMI as defined by the DMTF (Distributed Management Task Force) or it may be proprietary to the device.

The device will respond to the query. If the query was SNMP, the response will be an SNMP response and must be translated for our use. Similarly, if the query was a DMI query, the response will be as specified by the DMI standard and need to be translated for our use.

If the response indicates that any element of the external device has failed or in danger of failing, the program will set the corresponding alarm condition for that device.

Listed below in Table 1 are some typical specifications for an embodiment of the computer network and equipment monitoring system of the present invention. These ranges and specifications are illustrative only and can include different values and/or different parameters.

Table 1

Specifications:	
Temperature:	
Range:	-55°C to +125°C (-67°F to 257°F)
Sensor:	solid state element.
Accuracy:	+/-0.5° degree Celsius
Relative Humidity:	
Sensor:	porous ceramic, solid state.
Range:	30% to 90%
Accuracy:	10%
Response Time:	120 seconds
Air Speed:	
Range:	0 to 10 cubic feet/minute, non-linear.
Accuracy:	30%

Sensor:	hot-wire anemometer (thermistor bridge).
Housing:	powder coated, 16 gauge aluminum.
Color:	PMS 462 Light Blue, white lettering
Connectors:	
Ethernet:	RJ-45 to Cat 5 network wiring
Series:	RJ-11 to serial device (for installation setup),
Power:	6mm barrel jack for 5 vdc power.
Data Speed:	10mHz, Ethernet
Protocol:	TCP/IP
Web page Generation:	Netscape 4.0 and IE 4.0 compatible
E-mail format:	MIME, limited to 200 characters
Mounting:	By 6-38 wood screws (supplied) or double-sided tape corner mount (supplied).
Indicator Lights:	Power On, Temp out of limit, Humidity out-of-limit, Air Flow out-of-limit.
Web Page Fields Accepted by Form:	
Field 1:	"Room or company name"
Field 2:	"Contact"
Field 3:	"URL address"
Field 4:	"IP address"
Field 5:	"Primary e-mail address"
Field 6:	"Secondary e-mail address"
Field 7:	"Temperature High Limit Setting:"
Field 8:	"Temperature Low Setting:"
Field 9:	"Humidity High setting:"
Field 10:	"Air Flow High setting:"
Field 11:	"Air Flow Low Setting:"
Field 12:	"Time between routing e-mail reports:"
Web Page Fields Generated at access:	
Field 1:	Temperature (C)
Field 2:	Temperature (f):
Field 3:	Humidity:
Field 4:	Air Flow
Field 5:	Current High Temp Limit
Field 6:	"Room or company name"

Although the present invention has been described in detail herein with reference to the illustrative embodiments, it should be understood that the description is by way of example only and is not to be construed in a limiting sense. It is to be further understood, therefore, that numerous changes in the details of the embodiments of this invention and additional embodiments of this invention will be apparent to, and may be made by, persons of ordinary skill in the art having reference to this description. It is contemplated that all such changes and additional embodiments are within the spirit and true scope of this invention as claimed below.

CLAIMS

1. A system for monitoring a space and its contents over a network, comprising:

a microprocessor to provide processing and network connectivity capability;

one or more sensors to detect one or more physical parameters and generate one or more sensor signals representative of the detected physical parameters;

an analog-to-digital converter for converting one or more of the sensor signals to a digital format and to provide one or more corresponding digital signals to the microprocessor;

instructions for processing said sensor signals and corresponding digital signals and generating an alarm signal when any of the one or more physical parameters exceeds a corresponding threshold value;

at least one input/output port for communicating with the network;

one or more memory modules for storing system data;

a network based interface for providing programming instructions to the microprocessor and for receiving monitoring status and alarm information from the system; and

a power source to power the system.

2. The system of Claim 1, wherein the network is a global computer network.

3. The system Claim 2, wherein the global computer network is the Internet.

4. The system of Claim 1, wherein the network is an intranet.

5. The system of Claim 1, further comprising one or more connectors to interface with external devices.

6. The system of Claim 5, wherein the one or more connectors further comprise no more than one of each of an Ethernet connector, a serial connector, a power connector, and a phone line connector.

7. The system of Claim 6, wherein the Ethernet connector is an RJ-45 to Cat 5 or Cat 3 wiring connector, and wherein the serial connector is an RJ-11 connector.

8. The system of Claim 6, wherein said power source is the excess voltage provided by an Ethernet cable coupled to said Ethernet connector.

9. The system of Claim 1, wherein the network connectivity capability is via a telephone line.

10. The system of Claim 1, wherein the network connectivity capability is via an Ethernet interface, and wherein said Ethernet interface has compliant TCP/IP stacks.

11. The system of Claim 1, wherein the microprocessor is an embedded Java microprocessor.

12. The system of Claim 11, wherein the microprocessor is a tiny internet interface microprocessor.

13. The system of Claim 11, wherein the microprocessor operates on an embedded Java software platform.

14. The system of Claim 1, wherein the one or more sensors further comprise no more than one of each of a temperature sensor, a relative humidity sensor, and an air flow sensor.

15. The system of Claim 14, wherein the relative humidity sensor further comprises a Figaro Engineering NH-2 humidity sensor, and wherein the air flow sensor further comprises a hot-wire anemometer circuit.

16. The system of Claim 1, wherein the one or more physical parameters comprise temperature, relative humidity, and air flow.

17. The system of Claim 1, further comprising one or more indicator lights to indicate one or more system conditions.

18. The system of Claim 1 further comprising a radio frequency interface operable to communicate wirelessly with the network or with a device external to the network.

19. The system of Claim 1, further comprising instructions for generating and forwarding an email status report to one or more users.

20. The system of Claim19, wherein the status report indicates that one or more of the one or more physical parameters has exceeded said corresponding threshold value.

21. The system of Claim 1, further comprising instructions for generating and forwarding an email alarm report to one or more users when any one of the one or more physical parameters exceeds said corresponding threshold value.

22. The system of Claim 1, further comprising instructions for generating and forwarding a status report via electronic paging.

23. The system of Claim 1, wherein said programming instructions are provided in HTML.

24. The system of Claim 1, wherein said programming instructions comprise parameter threshold values.

25. The system of Claim 1, wherein said network based interface is an HTML interface.

26. The system of Claim 25, wherein said HTML interface comprises an image display area, a monitored parameter display area, an alarm threshold display area, and a system user information display area.

27. The system of Claim 26, wherein said system user information display area can be configured by a user to display customized information.

28. The system of Claim 1, further comprising a rechargeable backup battery to provide power upon loss of said power source.

29. The system of Claim 1, wherein said power source is a 5 volt DC power source.

30. The system of Claim 1, further comprising a video imager to provide a digital image of the space or its contents.

31. The system of Claim 30, wherein said video imager is a CMOS imager.

32. The system of Claim 30, wherein the system is mounted internal to a component rack for monitoring of individual components.

33. The system of Claim 30, further comprising a binary input to activate said video imager to capture a current image of the monitored space.

34. The system of Claim 33, further comprising an external sensor, wherein said external sensor provides said binary input upon the occurrence of a preset condition.

35. The system of Claim 34, wherein said external sensor is a magnetic switch for sensing the opening of a door to said space, and wherein said preset condition is the opening of said door.

36. The system of Claim 1, further comprising instructions for software agents operable to investigate the internal condition of network components.

37. The system of Claim 36, wherein said software agents investigate the internal condition of compatible network components through SNMP, DMI, and SMBIOS interfaces.

38. The system of Claim 1, further comprising one or more binary outputs connected to one or more relays to control one or more external loads, and instructions for controlling said outputs.

39. The system of Claim 38, wherein controlling comprises turning an external load on or off, and wherein the external load is an air conditioning unit.

40. The system of Claim 1, wherein said instructions for processing can be updated via the network based interface.

41. The system of Claim 1, further comprising a smoke alarm sensor for generating an alarm signal upon detecting an audible smoke alarm.

42. The system of Claim 1, further comprising a 64-bit encoder chip to provide encryption and password protection for said network based interface configurable by a user.

43. A system for monitoring a space and its contents over a network, comprising:

a microprocessor to provide processing and network connectivity capability;

a video imager to generate a digital image of the space or its contents;

instructions for processing said digital image and forwarding said digital image to the network;

at least one input/output port for communicating with the network;

one or more memory modules for storing system data;

a network based interface for providing programming instructions to the microprocessor and for receiving information from the system; and

a power source to power the system.

44. The system of Claim 43, wherein the network is a global computer network.

45. The system of Claim 44, wherein the global computer network is the Internet.

46. The system of Claim 43, wherein the network is an intranet.

47. The system of Claim 43, further comprising one or more connectors to interface with external devices.

48. The system of Claim 47, wherein the one or more connectors further comprise no more than one of each of an Ethernet connector, a serial connector, a power connector, and a phone line connector.

49. The system of Claim 47, wherein the Ethernet connector is an RJ-45 to Cat 5 or Cat 3 wiring connector.

50. The system of Claim 48, wherein said power source is the excess voltage provided by an Ethernet cable coupled to said Ethernet connector.

51. The system of Claim 43, wherein the network connectivity capability is via a telephone line.

52. The system of Claim 43, wherein the network connectivity capability is via an Ethernet interface, and wherein said Ethernet interface has compliant TCP/IP stacks.

53. The system of Claim 43, wherein the microprocessor is an embedded Java microprocessor.

54. The system of Claim 53, wherein the microprocessor is a tiny internet interface microprocessor.

55. The system of Claim 53, wherein the microprocessor operates on an embedded Java software platform.

56. A system for monitoring a space and its contents over a network, comprising:

a microprocessor to provide processing and network connectivity capability;

instructions for software agents operable to investigate the internal condition of network components and generate one or more component status signals;

instructions for processing said status signals and generating an alarm signal when any of the one or more component status signals exceeds a corresponding threshold value;

at least one input/output port for communicating with the network;

one or more memory modules for storing system data;

a network based interface for providing programming instructions to the microprocessor and for receiving information from the system; and

a power source to power the system.

57. The system of Claim 56, wherein said software agents investigate the internal condition of compatible network components through SNMP, DMI, and SMBIOS interfaces.

58. A method for monitoring a space and its contents over a network with an integrated network server, comprising the steps of:

providing processing and network connectivity capability with a microprocessor;

at one or more sensors, detecting one or more physical parameters;

generating at said sensors one or more sensor signals representative of the detected physical parameters;

converting one or more of the sensor signals to a digital format at an analog-to-digital converter and forwarding one or more corresponding digital signals to the microprocessor;

processing said sensor signals to generate an alarm signal when any of the one or more physical parameters exceeds a corresponding threshold value;

communicating monitoring data with the network through at least one input/output port;

providing programming instructions to the microprocessor through a network-based interface; and

transmitting space and content status information to a user.

59. The method of Claim 58, wherein the network is a global computer network.

60. The method of Claim 59, wherein the global computer network is the Internet.

61. The method of Claim 58, wherein the network is an intranet.

62. The method of Claim 58, further comprising the step of interfacing with one or more external devices with through one or more connectors.

63. The method of Claim 62, wherein the one or more connectors further comprise no more than one of each of an Ethernet connector, a serial connector, a power connector, and a phone line connector.

64. The method of Claim 63, wherein the Ethernet connector is an RJ-45 to Cat 5 or Cat 3 wiring connector, and wherein the serial connector is an RJ-11 connector.

65. The method of Claim 64, further comprising the step of powering said network server with the excess voltage provided by an Ethernet cable coupled to said Ethernet connector.

66. The method of Claim 58, wherein the network connectivity capability is via a telephone line.

67. The method of Claim 58, wherein the network connectivity capability is via an Ethernet interface, and wherein said Ethernet interface has compliant TCP/IP stacks.

68. The method of Claim 58, wherein the microprocessor is an embedded Java microprocessor.

69. The method of Claim 68, wherein the microprocessor is a tiny internet interface microprocessor.

70. The method of Claim 68, wherein the microprocessor operates on an embedded Java software platform.

71. The method of Claim 58, further comprising the step of generating and forwarding an email status report to one or more users through said network-based interface.

72. The method of Claim 71, wherein the status report indicates that one or more of the one or more physical parameters has exceeded said corresponding threshold value.

73. The method of Claim 58, further comprising the steps of generating and forwarding an email alarm report to one or more users when any one of the one or more physical parameters exceeds said corresponding threshold value.

74. The method of Claim 58, further comprising the steps of generating and forwarding a status report via electronic paging.

75. The method of Claim 58, wherein said programming instructions are provided in HTML.

76. The method of Claim 58, wherein said programming instructions comprise parameter threshold values.

77. The method of Claim 58, wherein said network-based interface is an HTML interface.

78. The method of Claim 77, wherein said HTML interface comprises an image display area, a monitored parameter display area, an alarm threshold display area, and a system user information display area.

79. The method of Claim 78, wherein said system user information display area can be configured by a user to display customized information.

80. The method of Claim 58, further comprising the steps of generating a digital image of the space or its contents with a video imager.

81. The method of Claim 80, wherein said video imager is a CMOS imager.

82. The method of Claim 80, wherein the network server is mounted internal to a component rack for monitoring of individual components.

83. The method of Claim 80, further comprising the step of activating said video imager to capture a current image of the monitored space using a binary input.

84. The method of Claim 83, further comprising the step of generating said binary input at an external sensor upon the occurrence of a preset condition.

85. The method of Claim 58, further comprising the step of investigating the internal condition of network components using software agents.

86. The method of Claim 85, wherein said software agents investigate the internal condition of compatible network components through SNMP, DMI, and SMBIOS interfaces.

87. The method of Claim 58, further comprising the step of controlling one or more external loads using one or more binary outputs connected to one or more relays.

88. The method of Claim 87, wherein the step of controlling comprises turning an external load on or off.

89. The method of Claim 58, further comprising the step of updating said instructions for processing via the network-based interface.

90. The method of Claim 58, further comprising the step of generating an alarm signal using a smoke alarm sensor upon detecting an audible smoke alarm.

91. The method of Claim 58, further comprising the step of providing user configurable encryption and password protection for said network-based interface using a 64-bit encoder chip.

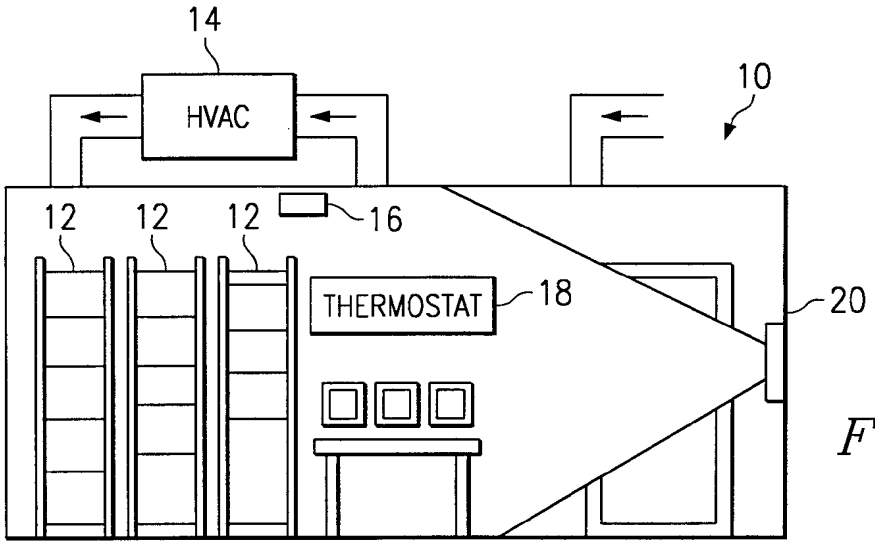


FIG. 1

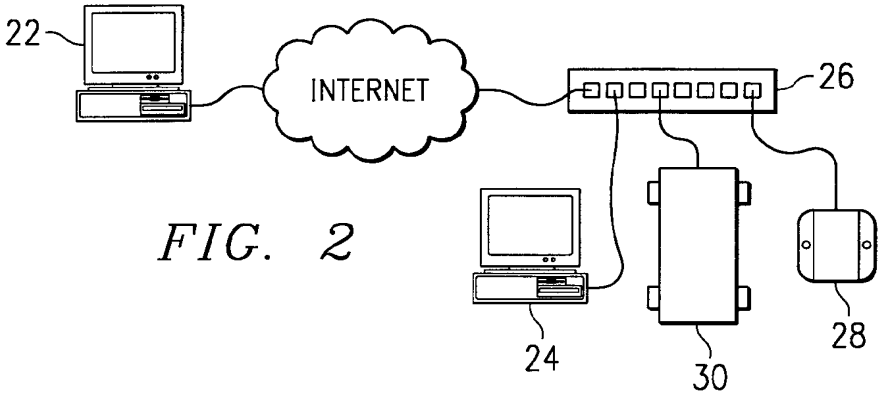


FIG. 2

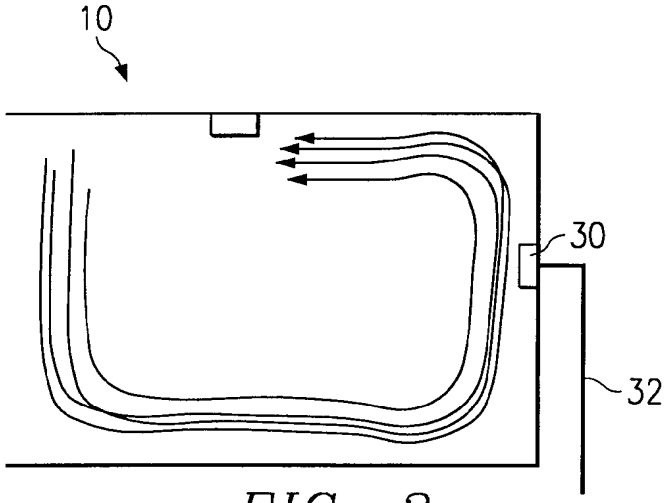


FIG. 3

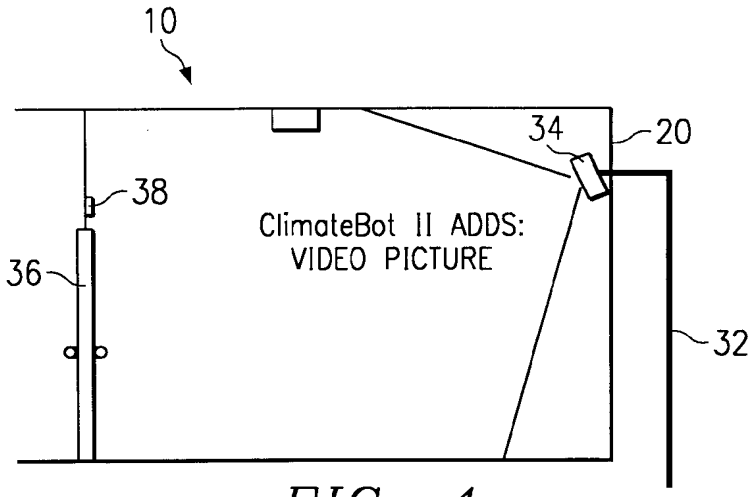


FIG. 4

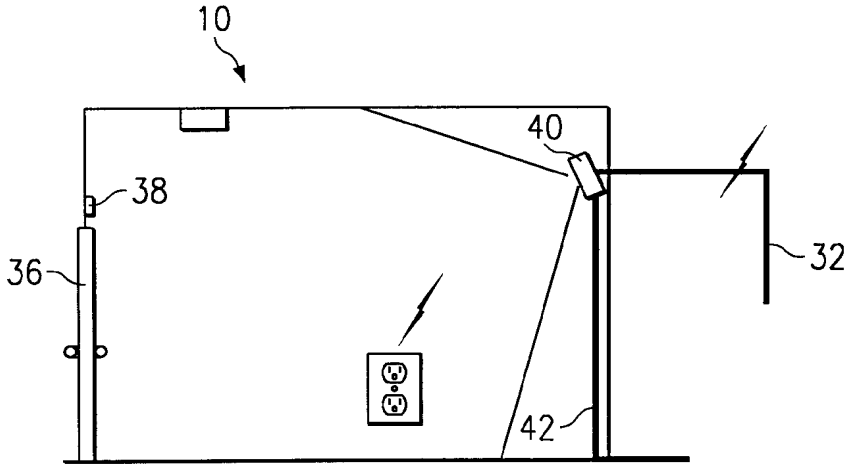


FIG. 5

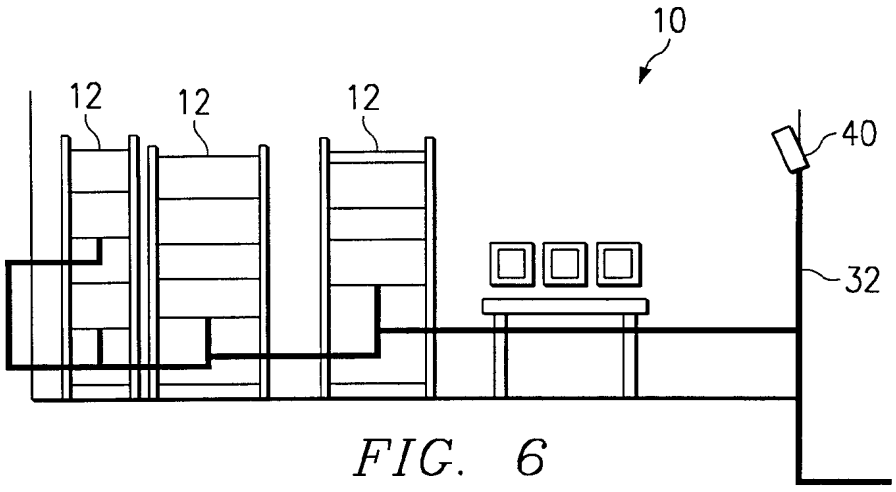


FIG. 6

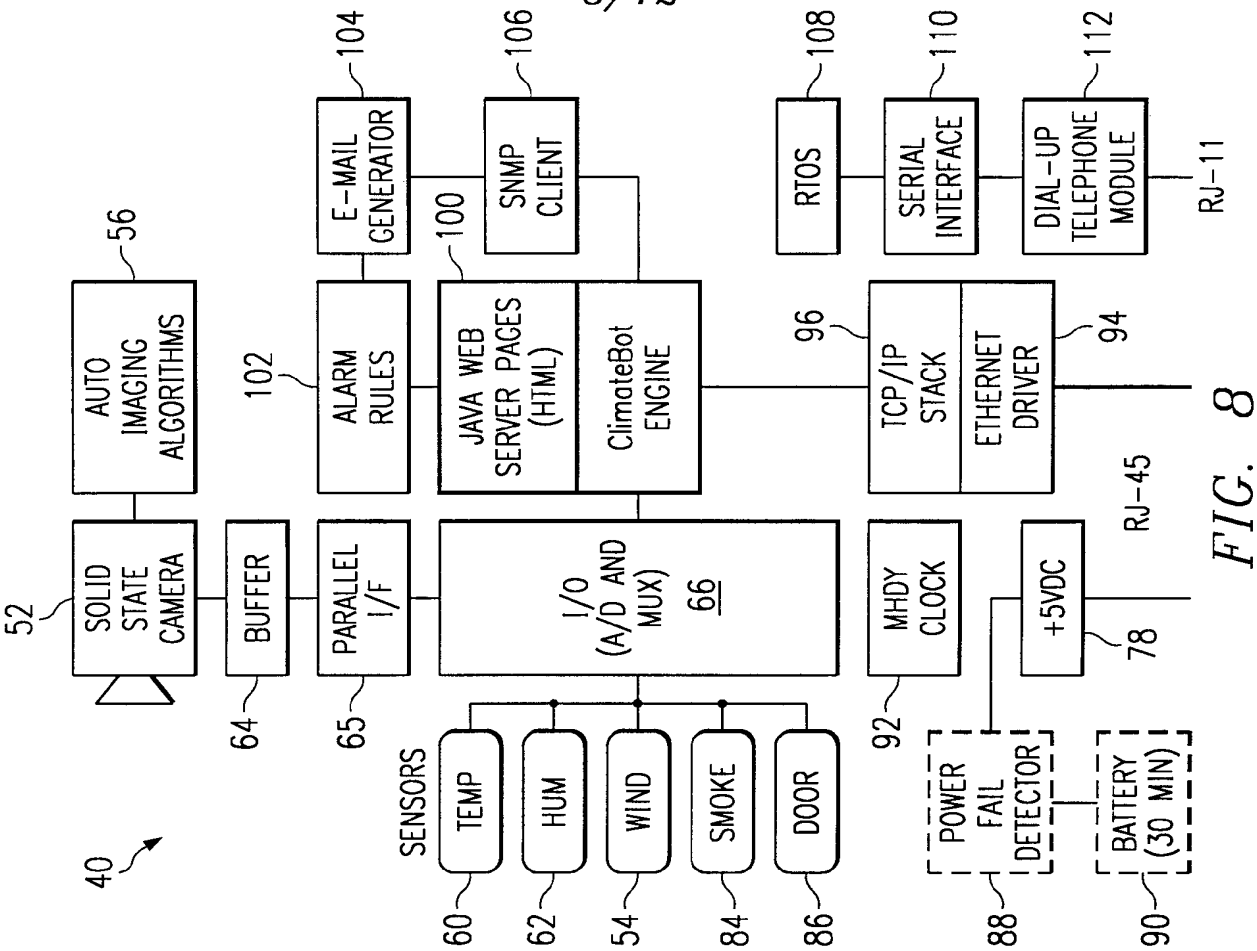

40
52
SOLID STATE CAMERA
56
AUTO IMAGING ALGORITHMS
64
BUFFER
65
PARALLEL I/F
I/O (A/D AND MUX) 66
SENSORS
60
TEMP
62
HUM
54
WIND
84
SMOKE
86
DOOR
92
MHDY CLOCK
88
POWER FAIL DETECTOR
90
BATTERY (30 MIN)
78
+5VDC
RJ-45
102
ALARM RULES
100
JAVA WEB SERVER PAGES (HTML)
ClimateBot ENGINE
104
E-MAIL GENERATOR
106
SNMP CLIENT
96
TCP/IP STACK
ETHERNET DRIVER
94
108
RTOS
110
SERIAL INTERFACE
112
DIAL-UP TELEPHONE MODULE
RJ-11

FIG. 8

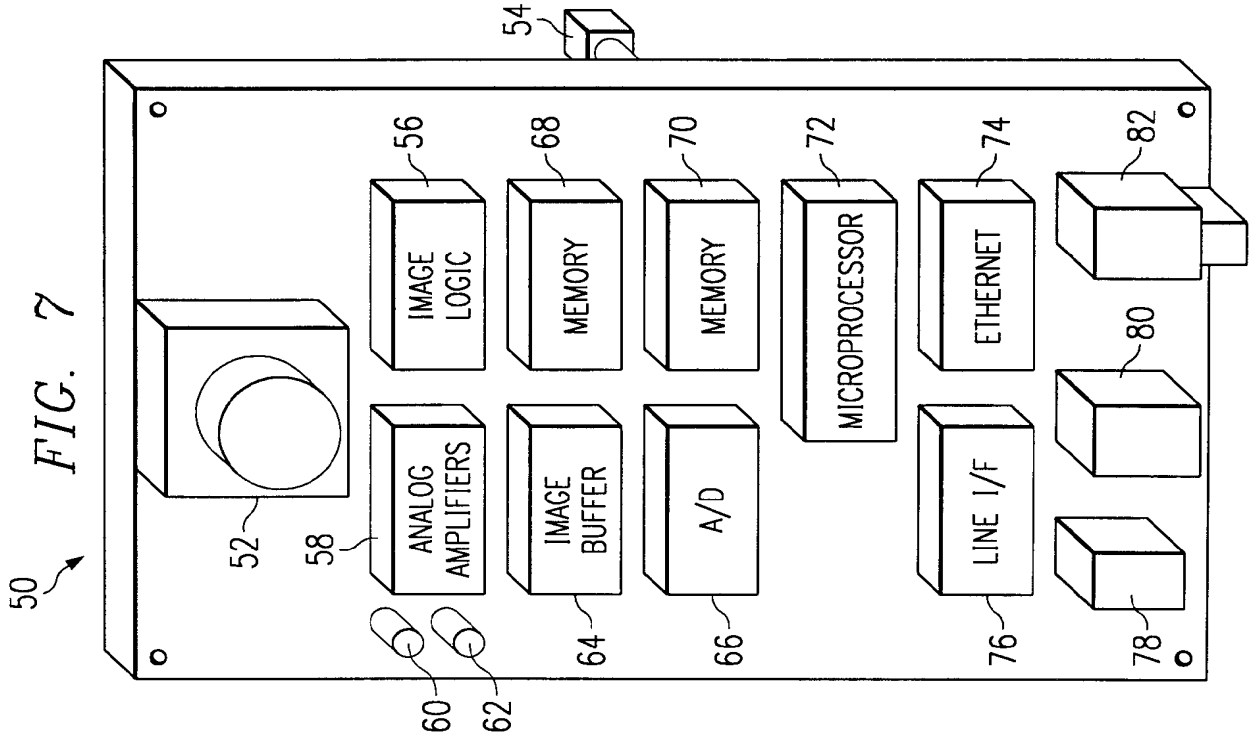

50
52
54
56
IMAGE LOGIC
58
ANALOG AMPLIFIERS
60
62
64
IMAGE BUFFER
66
A/D
68
MEMORY
70
MEMORY
72
MICROPROCESSOR
74
ETHERNET
76
LINE I/F
78
80
82

FIG. 7

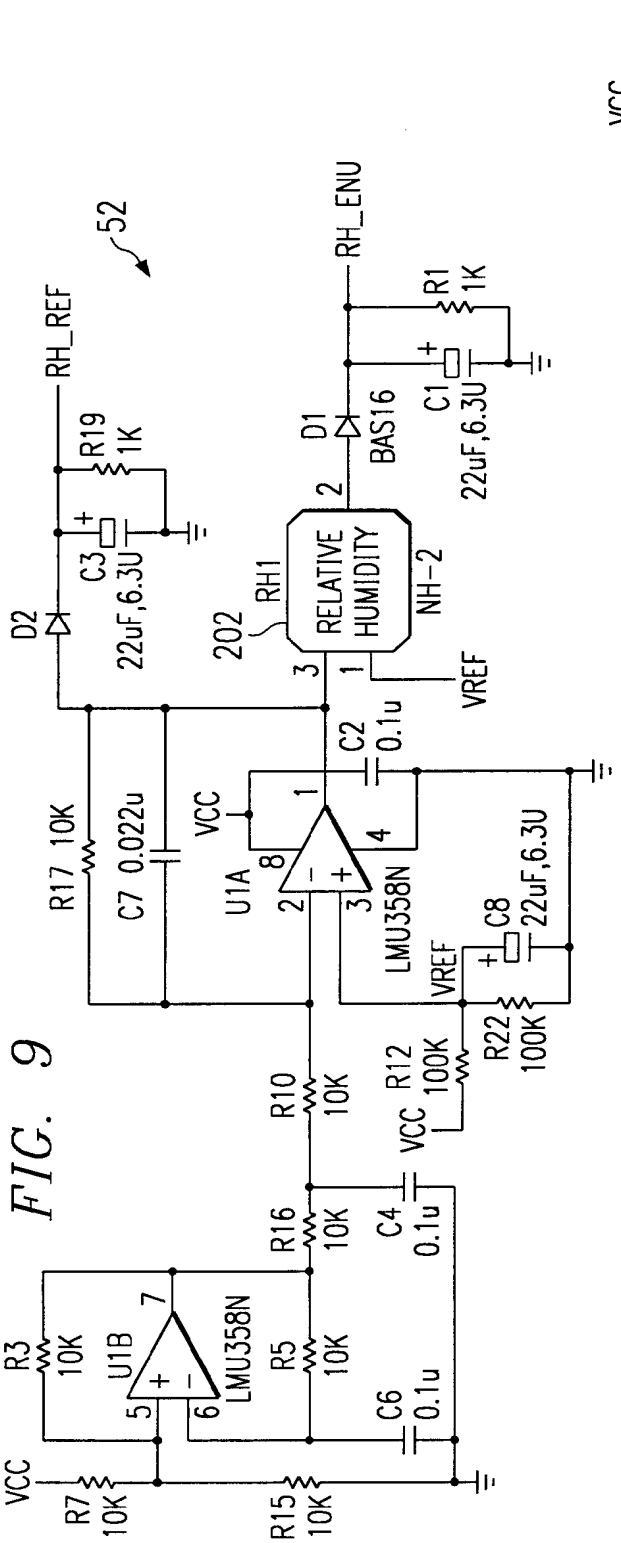

52
RH_REF
RH_ENU
R19 1K
R1 1K
C3 22uF,6.3U
C1 22uF,6.3U
D2
D1 BAS16
202
RH1
RELATIVE HUMIDITY
NH-2
VREF
C2 0.1u
R17 10K
C7 0.022u
VCC
U1A
LMU358N
C8 22uF,6.3U
VREF
R22 100K
R12 100K
R10 10K
R16 10K
C4 0.1u
R3 10K
U1B
LMU358N
R5 10K
C6 0.1u
R7 10K
R15 10K

FIG. 9

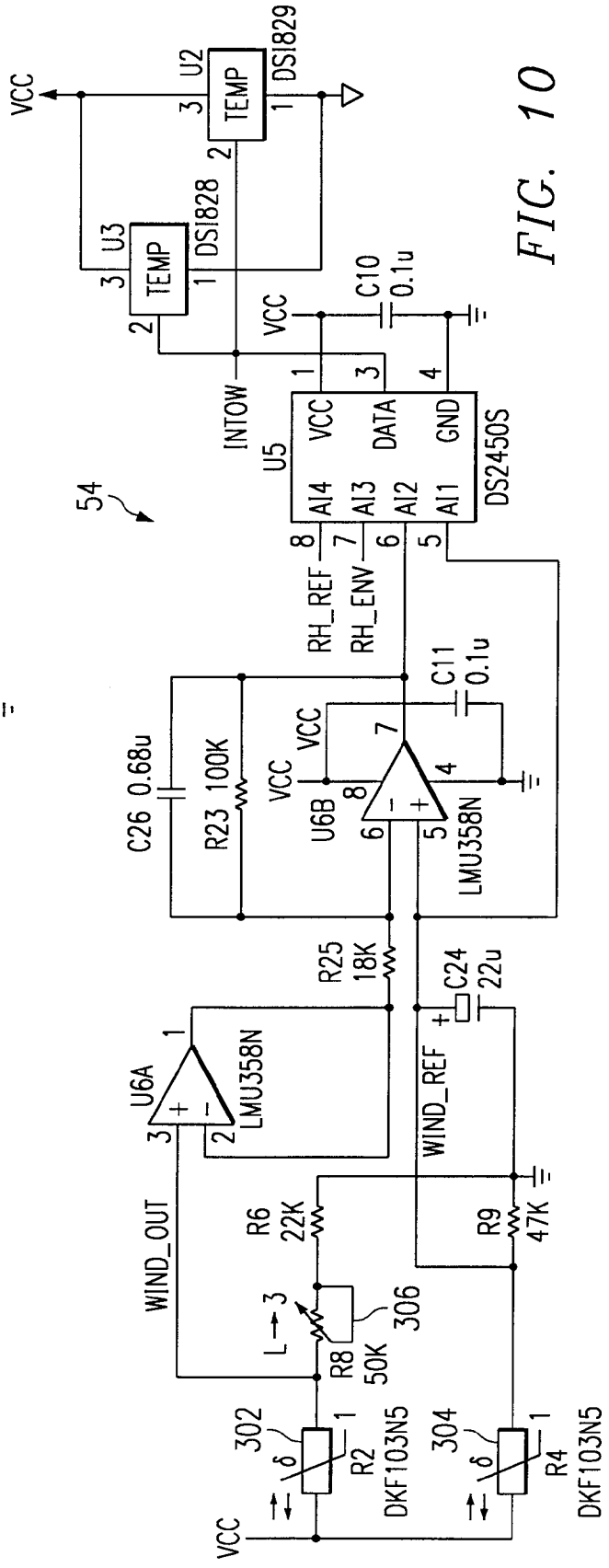

VCC
U2 TEMP DSI829
U3 TEMP DSI828
C10 0.1u
INTOW
U5 DS2450S
VCC DATA GND
AI4 AI3 AI2 AI1
54
RH_REF
RH_ENV
C11 0.1u
C26 0.68u
R23 100K
U6B
LMU358N
R25 18K
C24 22u
U6A
LMU358N
WIND_REF
WIND_OUT
R6 22K
R9 47K
L→3
R8 50K
306
302
R2 DKF103N5
304
R4 DKF103N5

FIG. 10

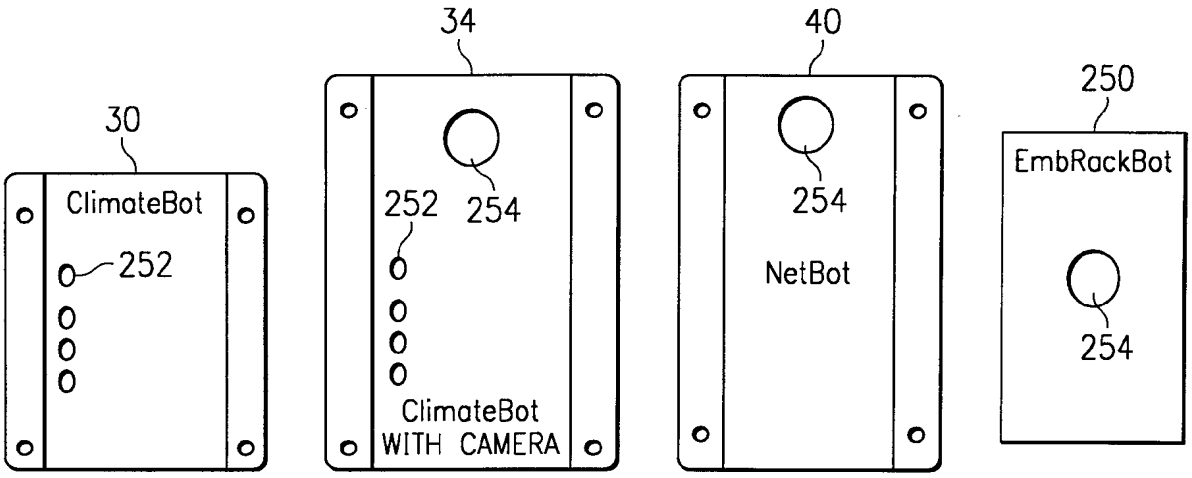


FIG. 11

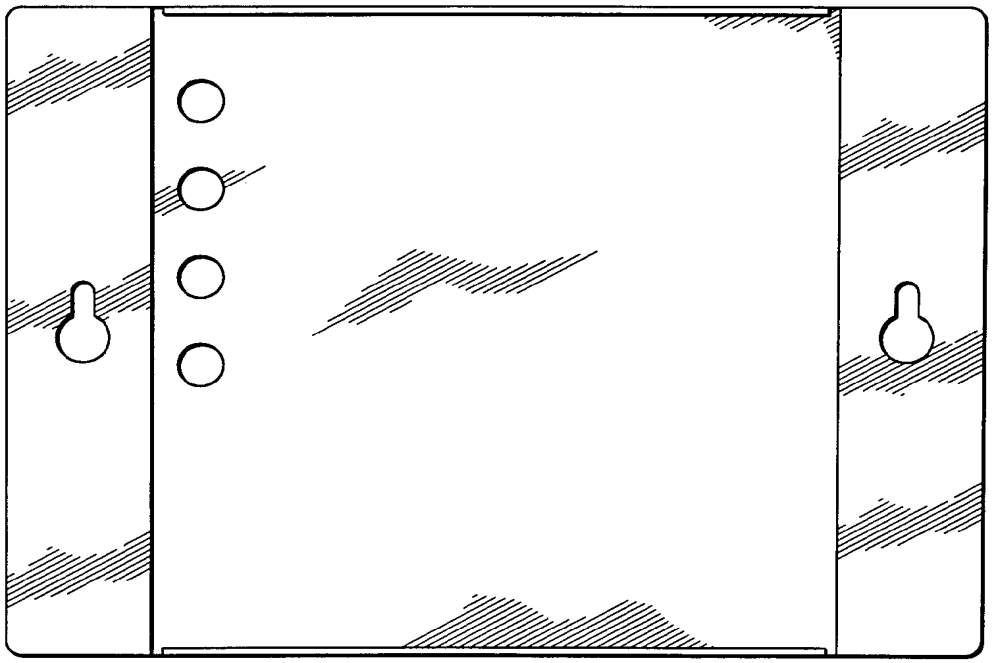


FIG. 12A

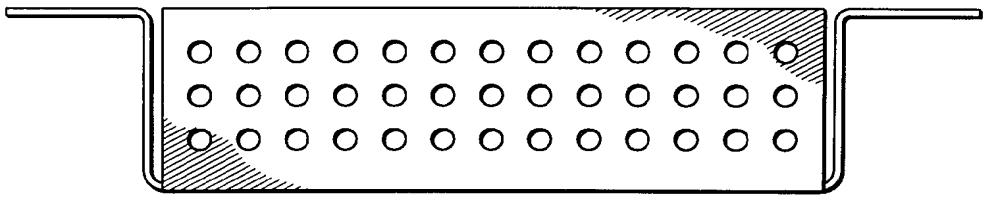


FIG. 12B

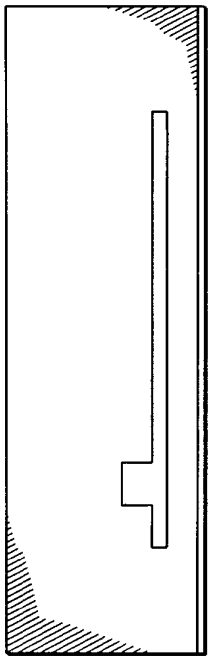


FIG. 12C

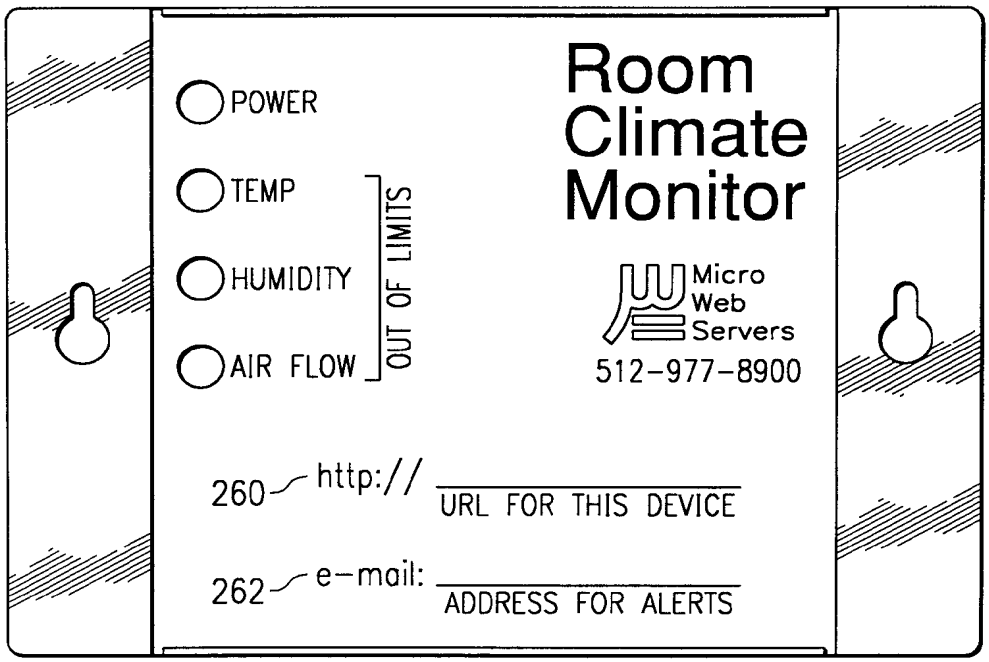
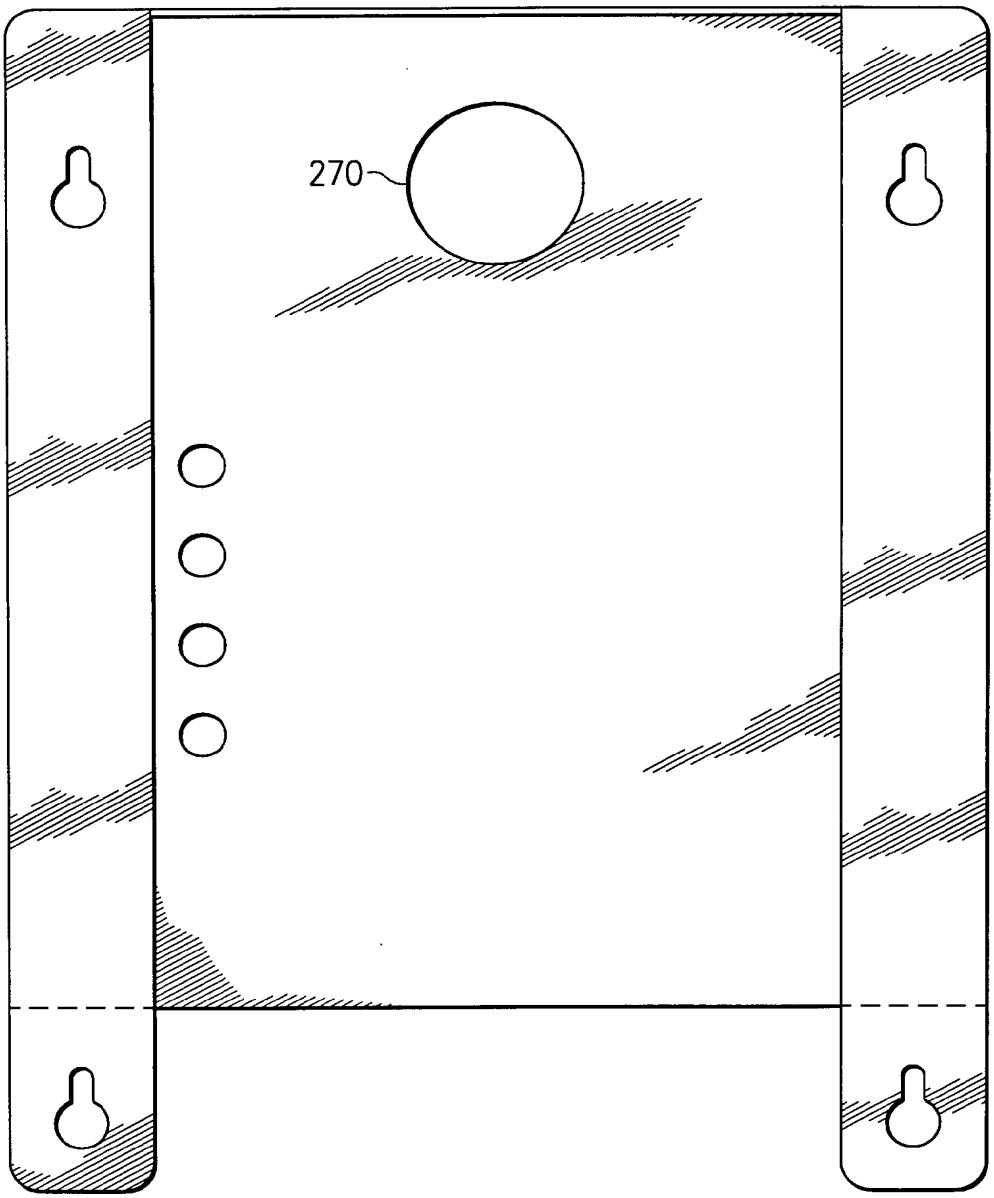


FIG. 12D

FIG. 13A



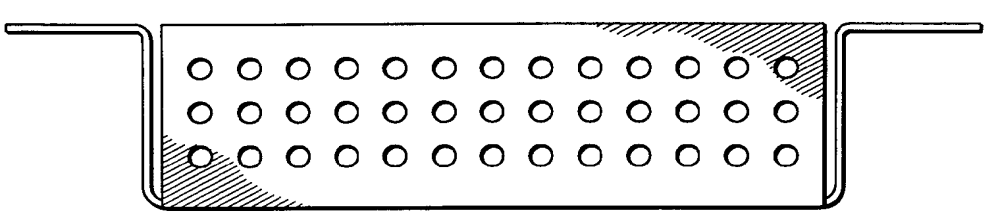


FIG. 13B

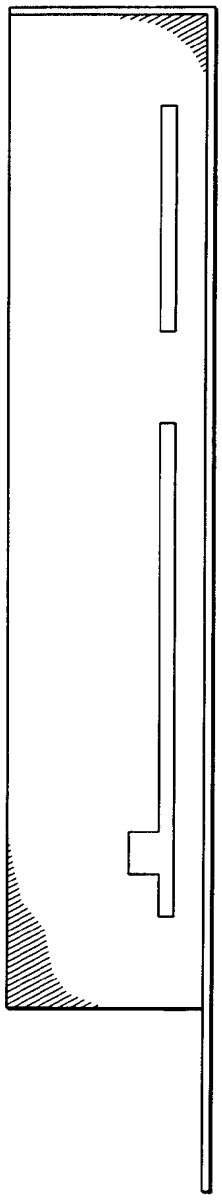


FIG. 13C

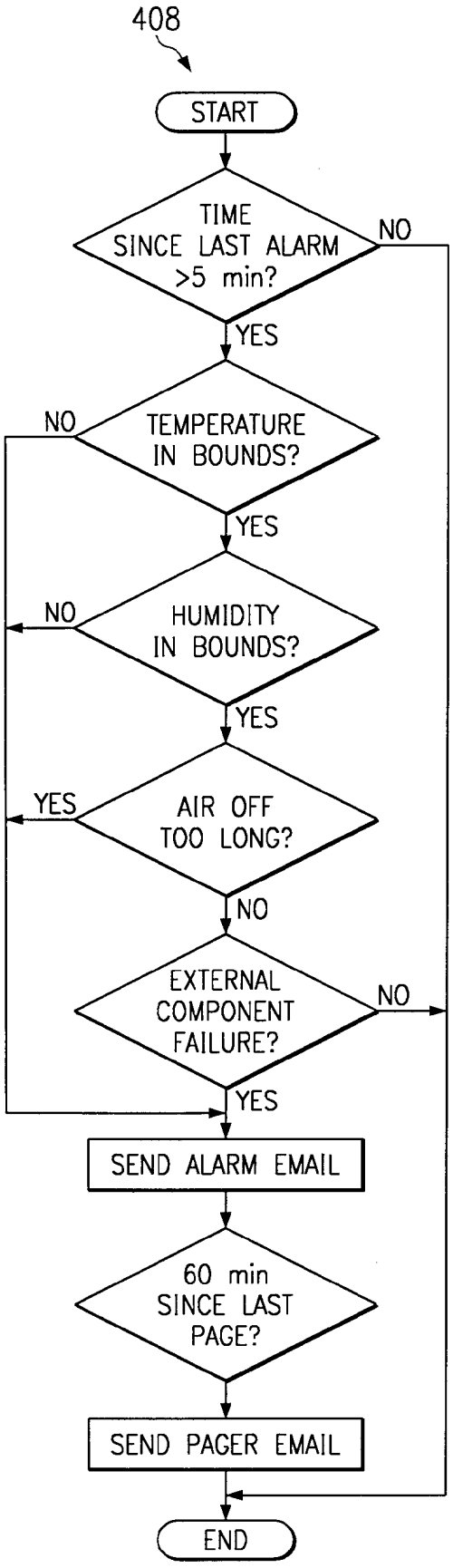


FIG. 14A

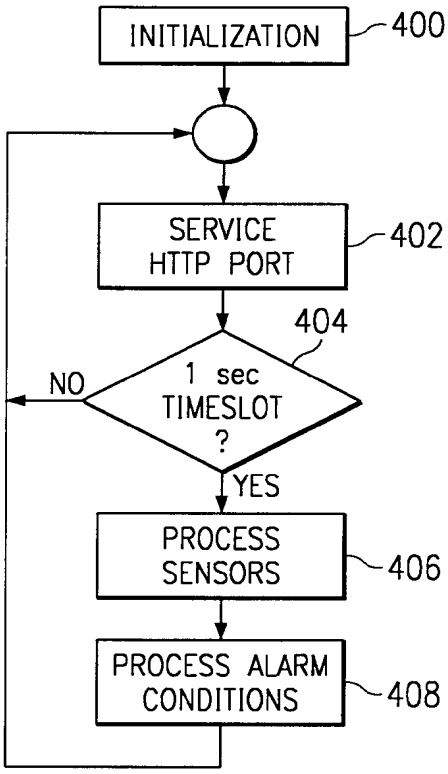


FIG. 14

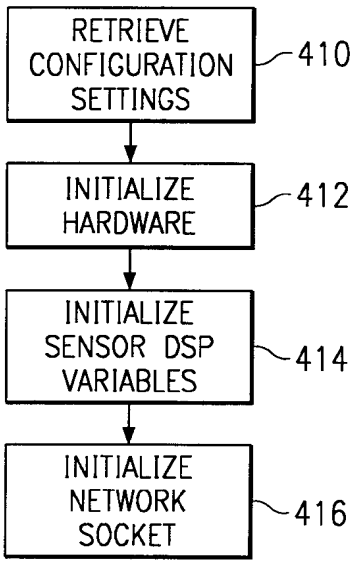


FIG. 15

FIG. 16

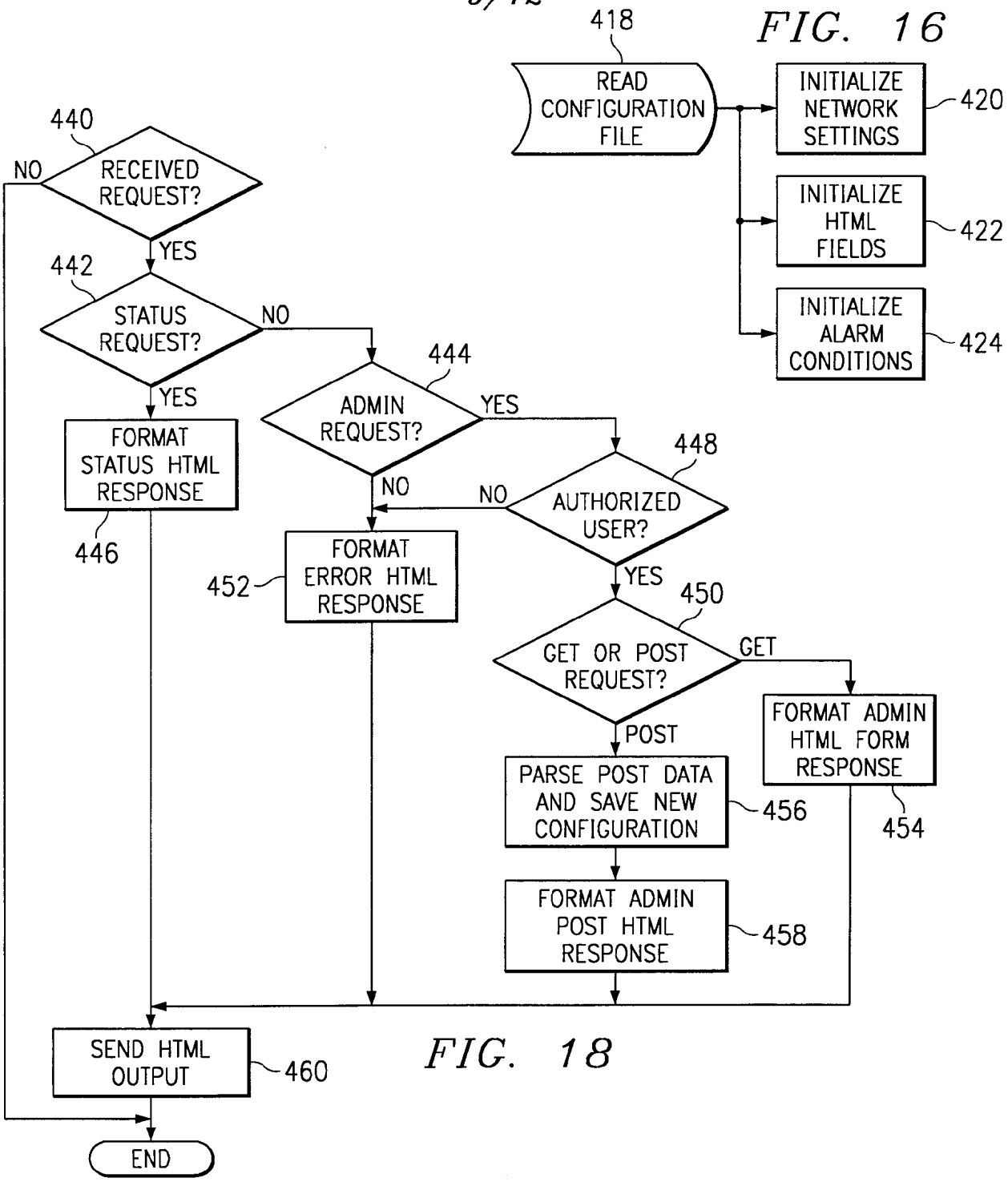


FIG. 18

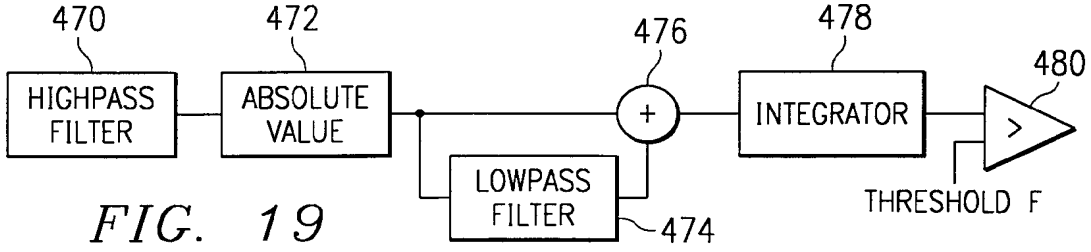


FIG. 19

NetBotz CoreTex –

URL: http://www.coretex.com/~thompson

Date, time:	7/22/99 08:00
Temp (C):	22.1
Temp (F)	72.6
Humidity (%)	55
Air Flow (0–100)	6
Smoke Alarm Sound	Off

Limit Settings	High	Low
Temperature (C)	23	15
Humidity (%)	75	35
Air Flow (0–100)	1	90
Smoke Alarm	On	On

Equipment report (launched Bot returns):

Server "High Plains" Compaq	Status	Alarms?	Limit High	Limit Low
CPU Temp F	77		120	50
CPU Fan	1200		1400	1200
Disk Status	On		Off	Off
Router "Franks Favorite" 41B				
Temp	85		90	110
Data Lines Up?	On			Off
Server "High Plains" Compaq				
CPU Temp	80		120	50
CPU Fan	1300		1400	1200
Disk Status	On		Off	Off
UnPowerSup "Big Bertha" ACX 500				
On-line?	True		False	False
Charge capacity (%)	95	Yes	100	99
Server "Old Guy" Dell 4000				
CPU Temp	90		120	50
Disk Status	On		Off	Off

Destinations for Alarm e-mail and paging

E-Mail	
Primary:	itstaff@coretex.com; gerryc@flash.net
Secondary:	jnorton@flash.net
Paging:	5127896565@mail.att.net

FIG. 17

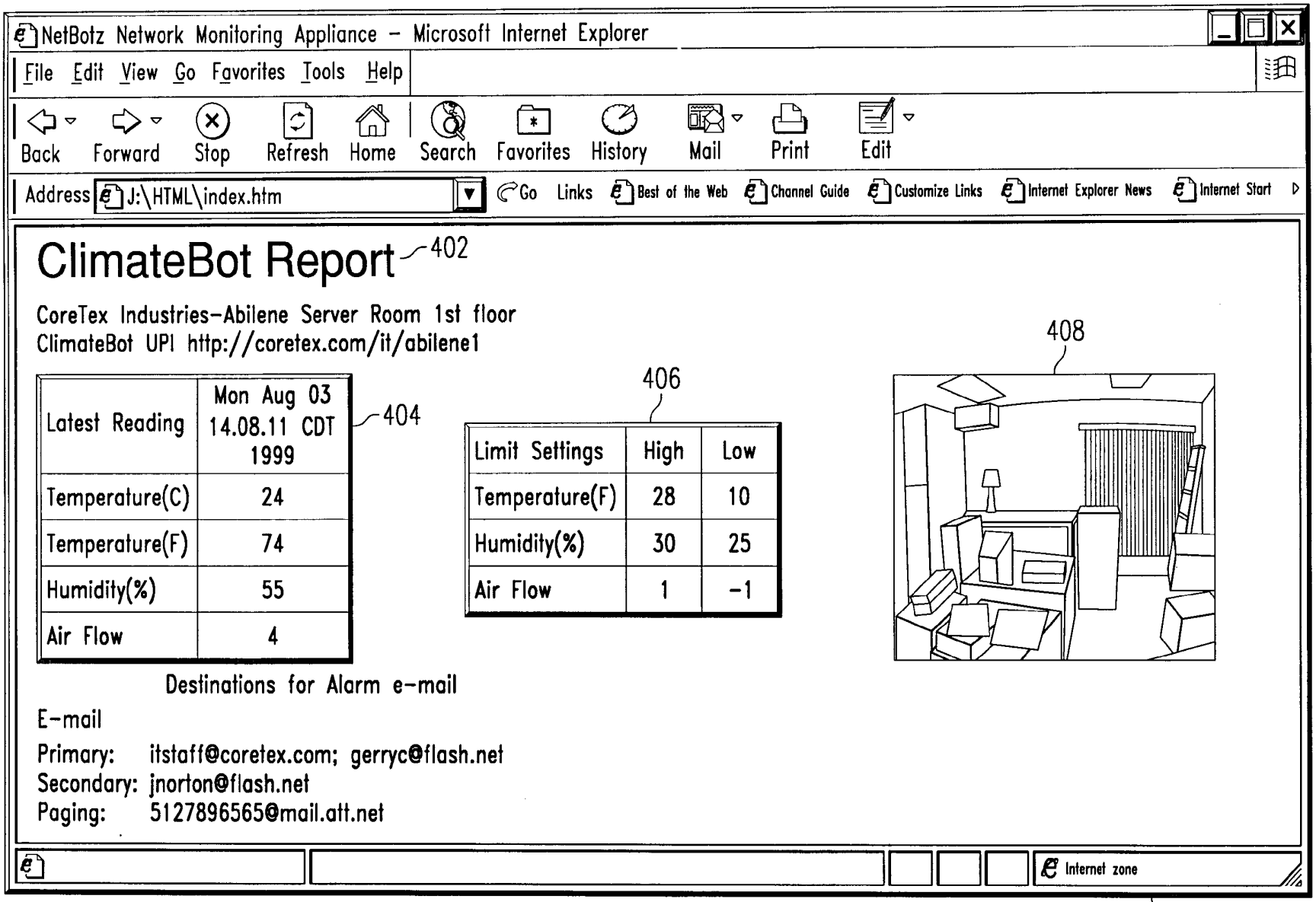

NetBotz Network Monitoring Appliance - Microsoft Internet Explorer
File Edit View Go Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit
Address J:\HTML\index.htm
Go Links Best of the Web Channel Guide Customize Links Internet Explorer News Internet Start
ClimateBot Report
402
CoreTex Industries-Abilene Server Room 1st floor
ClimateBot UPI http://coretex.com/it/abilene1
408
406
404
Latest Reading | Mon Aug 03 14.08.11 CDT 1999
Temperature(C) | 24
Temperature(F) | 74
Humidity(%) | 55
Air Flow | 4
Limit Settings | High | Low
Temperature(F) | 28 | 10
Humidity(%) | 30 | 25
Air Flow | 1 | -1
Destinations for Alarm e-mail
E-mail
Primary: itstaff@coretex.com; gerryc@flash.net
Secondary: jnorton@flash.net
Paging: 5127896565@mail.att.net
Internet zone
400

FIG. 20

Typical Scheduled E-mail Report

From: Abilene Server Room [SMTP:abilene@coretex.net]
Sent: Friday, July 09, 1999 08:00 AM
To: itstaff@coretex.com; hjones@flash.net
Subject: ClimateBot Report: Abilene Room Conditions

Temperature: 18C (64F)
Humidity: 55%
Air Flow: 50
Condition: within limits

Current Limit settings:
Temp (C) high: 20 Temp low: 15
Humidity high: 60 Humidity low: 40
Air flow high: 08 Air flow low: 00

To change limits and reporting go to: http://coretex.com/it/abilene1

FIG. 21A

Alarm Message (Typical)

From: Abilene Server Room [SMTP:abilene@coretex.net]
Sent: Friday, July 09, 1999 10:30 AM
To: itstaff@coretex.com; hjones@flash.net
Subject: Abilene Room Conditions

Temperature: 25C (75F) Above limits
Humidity: 55%
Air Flow: 50
Condition: Over temperature alarm

To change limits and reporting go to: http://coretex.com/it/abilene1

FIG. 21B

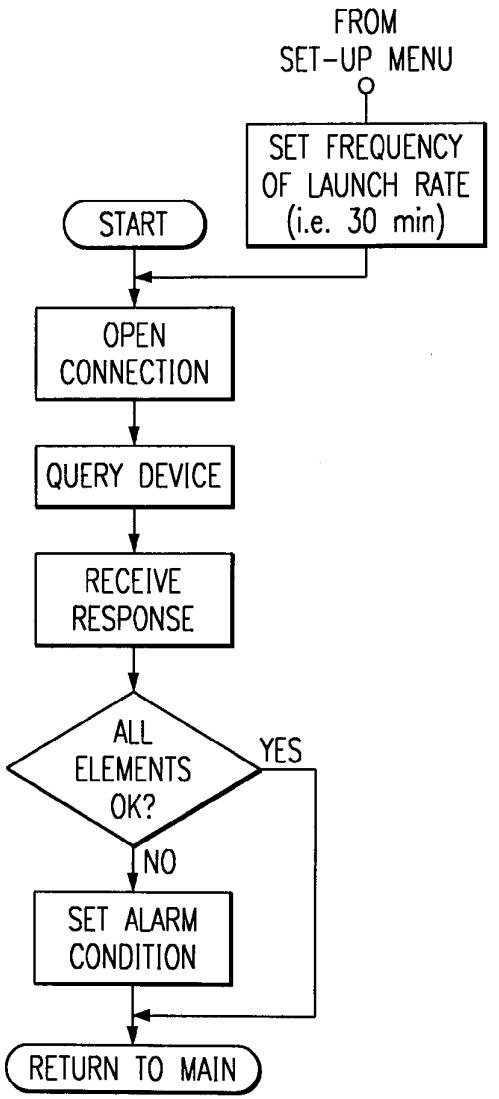


FIG. 22

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/US 00/29689

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G05B H04N G08B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, EPO-Internal, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 955 946 A (BEHESHTI ALI ET AL) 21 September 1999 (1999-09-21)	1,2,5-7, 9-11,13, 14,16, 17,24, 36,37, 56-59, 62-64, 66-68, 70,76, 85-87
Y	column 1, line 20 - line 43 column 2, line 57 -column 3, line 2 column 3, line 29 -column 4, line 52 column 7, line 53 -column 8, line 46 -/--	3,4, 19-23, 72,74, 77,78, 88,89

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 February 2001	28/02/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	De la Cruz Valera, D

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int. tional Application No
PCT/US 00/29689

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
	column 8, line 47 - line 51 figures 2,10,13	
Y	WO 99 15950 A (DEGRAFT JOHNSON JAMES ;FRANKLIN PAUL GLENN (US); HOLFORD WILLIAM C) 1 April 1999 (1999-04-01) page 4, line 3 - line 33 page 26, line 7 - line 29 page 32, line 28 -page 33, line 21 page 35, line 8 - line 22 figure 4	3,4, 19-23, 72,74, 77,78, 88,89
X	US 5 581 478 A (CRUSE MICHAEL ET AL) 3 December 1996 (1996-12-03) column 1, line 11 -column 2, line 20	1,58
X	US 5 229 850 A (TOYOSHIMA KEIICHI) 20 July 1993 (1993-07-20) the whole document	43,47,48
A	SINETICA CORP: "NEWSLETTER, ISSUE ONE 99" 'Online! February 1999 (1999-02) , SINETICA , UK XP002160504 Retrieved from the Internet: <URL: www.sinetica.co.uk> 'retrieved on 2001-02-15! the whole document	1-91
P,A	SINETICA CORP: "Netcom TH. Advanced SNMP Agent with web browser support" 'Online! April 2000 (2000-04) , SINETICA , UK XP002160505 Retrieved from the Internet: <URL: www.sinetica.co.uk> 'retrieved on 2001-02-15! the whole document	1-91

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

In ational Application No
PCT/US 00/29689

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5955946 A	21-09-1999	NONE	
WO 9915950 A	01-04-1999	AU 1062499 A	12-04-1999
		AU 9582798 A	12-04-1999
		AU 9582998 A	12-04-1999
		AU 9583198 A	12-04-1999
		AU 9583298 A	12-04-1999
		AU 9583398 A	12-04-1999
		AU 9583598 A	12-04-1999
		AU 9583698 A	12-04-1999
		AU 9584098 A	12-04-1999
		AU 9666398 A	12-04-1999
		AU 9667198 A	12-04-1999
		AU 9667298 A	12-04-1999
		AU 9667598 A	12-04-1999
		AU 9667698 A	12-04-1999
		AU 9667898 A	12-04-1999
		AU 9667998 A	12-04-1999
		AU 9668098 A	12-04-1999
		AU 9668298 A	03-05-1999
		AU 9777098 A	12-04-1999
		AU 9777298 A	12-04-1999
		AU 9777398 A	12-04-1999
		EP 1015995 A	05-07-2000
		EP 1015970 A	05-07-2000
		EP 1015986 A	05-07-2000
		WO 9915984 A	01-04-1999
		WO 9915960 A	01-04-1999
		WO 9916230 A	01-04-1999
		WO 9915974 A	01-04-1999
		WO 9915975 A	01-04-1999
		WO 9916206 A	01-04-1999
		WO 9916198 A	01-04-1999
		WO 9915977 A	01-04-1999
		WO 9916207 A	01-04-1999
		WO 9915988 A	01-04-1999
		WO 9915996 A	01-04-1999
		WO 9916002 A	01-04-1999
		WO 9916218 A	01-04-1999
		WO 9916099 A	01-04-1999
		WO 9915989 A	01-04-1999
		WO 9915978 A	01-04-1999
		WO 9915979 A	01-04-1999
		WO 9916202 A	01-04-1999
		WO 9919803 A	22-04-1999
		WO 9916203 A	01-04-1999
		US 6115040 A	05-09-2000
		US 6032184 A	29-02-2000
US 5581478 A	03-12-1996	US 5793646 A	11-08-1998
US 5229850 A	20-07-1993	JP 4086086 A	18-03-1992
		CA 2048076 A,C	31-01-1992